

NETGEAR 7000 Series Managed Switch Administration Guide

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10194-02
May 2006

Trademarks

NETGEAR and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc..

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders. Portions of this document are copyright Intoto, Inc.

May 2006

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

EN 55 022 Declaration of Conformance

This is to certify that the 7000 Series Managed Switch is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Certificate of the Manufacturer/Importer

It is hereby certified that the 7000 Series Managed Switch has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das 7000 Series Managed Switch gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.



Note: Delete this note and the information below for products that are not wireless.

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter."

Declaration Of Conformity

We NETGEAR, Inc., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model 7xxx Cardbus Card Wireless Adapter complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

NOTE: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

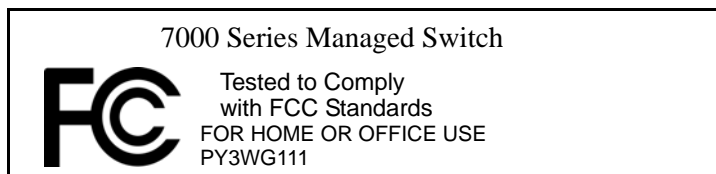
FCC Requirements for Operation in the United States

Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected

- Consult the dealer or an experienced radio/TV technician for help.



Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (7000 Series Managed Switch) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Canada ID: 4054A-WG111

Product and Publication Details

Model Number:	7xxx
Publication Date:	May 2006
Product Family:	Managed Switch
Product Name:	7000 Series Managed Switch
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10194-02
Publication Version Number:	1.1

Contents

NETGEAR 7000 Series Managed Switch Administration Guide

About This Book	xi
-----------------------	----

Chapter 1

Getting Started

In-band and Out-of-band Connectivity	1-1
Configuring for In-band Connectivity	1-1
Using BootP or DHCP	1-1
Using the EIA-232 Port	1-2
Configuring for Out-Of-Band Connectivity	1-3
Starting the Switch	1-4
Initial Configuration	1-4
Initial Configuration Procedure	1-5
Software Installation	1-6
Quick Starting the Networking Device	1-6
System Information and System Setup	1-6

Chapter 2

Using the Web Interface

Configuring for Web Access	2-1
Starting the Web Interface	2-2
Web Page Layout	2-2
Configuring an SNMP V3 User Profile	2-2
Command Buttons	2-3

Chapter 3

Virtual LANs

VLAN Configuration Example	3-2
CLI Examples	3-2
Example #1: Create Two VLANs	3-2
Example #2: Assign Ports to VLAN2	3-3

Example #3: Assign Ports to VLAN3	3-3
Example #4: Assign VLAN3 as the Default VLAN	3-3
Graphical User Interface	3-4
Chapter 4 Link Aggregation	
CLI Example	4-1
Example 1: Create two LAGS:	4-3
Example 2: Add the ports to the LAGs:	4-4
Example 3: Enable both LAGs.	4-4
Chapter 5	
IP Routing Services	
Port Routing	5-1
Port Routing Configuration	5-2
CLI Examples	5-3
Example 1. Enabling routing for the Switch	5-3
Example 2. Enabling Routing for Ports on the Switch	5-4
VLAN Routing	5-4
VLAN Routing Configuration	5-5
CLI Examples	5-5
Example 1: Create Two VLANs	5-6
Example 2: Set Up VLAN Routing for the VLANs and the Switch.	5-6
VLAN Routing RIP Configuration	5-7
CLI Example	5-8
VLAN Routing OSPF Configuration	5-10
CLI Example	5-10
Routing Information Protocol	5-12
RIP Configuration	5-12
CLI Example	5-13
Example #1: Enable Routing for the Switch:	5-13
Example #2: Enable Routing for Ports	5-14
Example #3. Enable RIP for the Switch	5-14
Example #4. Enable RIP for ports 1/0/2 and 1/0/3	5-15
OSPF	5-15
CLI Examples	5-16
Example #1 Configuring an Inter-Area Router	5-17
Example #2 - Configuring OSPF on a Border Router	5-19

Proxy Address Resolution Protocol (ARP)	5-21
Overview	5-21
CLI Examples	5-22
Example #1: show ip interface	5-22
Example #2: ip proxy-arp	5-22
Chapter 6	
Virtual Router Redundancy Protocol	
CLI Examples	6-2
Chapter 7	
Access Control Lists (ACLs)	
Overview	7-1
Limitations	7-1
MAC ACLs	7-1
Configuring IP ACLs	7-2
Process	7-3
IP ACL CLI Example	7-3
MAC ACL CLI Examples	7-4
Example #1: mac access list	7-5
Example #2: permit any	7-6
Example #3 Configure mac access-group	7-7
Example #4 permit	7-8
Example #5: show mac access-lists	7-9
Chapter 8	
Class of Service (CoS) Queuing	
Overview	8-1
CoS Queue Mapping	8-1
Trusted Ports	8-1
Untrusted Ports	8-2
CoS Queue Configuration	8-2
Port Egress Queue Configuration	8-2
Drop Precedence Configuration (per Queue)	8-3
Per Interface Basis	8-3
CLI Examples	8-3
Example #1: show classofservice trust	8-4

Example #2: set classofservice trust mode	8-4
Example #3: show classofservice ip-precedence mapping	8-5
Example #4: Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode	8-5
Example #5: Set CoS Trust Mode of an Interface	8-6
Traffic Shaping	8-6
CLI Example	8-6
Example #1 traffic-shape	8-7
Chapter 9	
Differentiated Services	
CLI Example	9-2
DiffServ for VoIP Configuration Example	9-4
Chapter 10	
IGMP Snooping	
Overview	10-1
CLI Examples	10-1
Example #1: Enable IGMP Snooping	10-1
Example #2: show igmpsnooping	10-2
Example #3: show mac-address-table igmpsnooping	10-2
Chapter 11	
Port Security	
Overview	11-1
Operation	11-2
CLI Examples	11-3
Example #1: show port security	11-3
Example #2: show port security on a specific interface	11-3
Example #3: (Config) port security	11-3
Chapter 12	
Traceroute	
CLI Example	12-2
Chapter 13	
Configuration Scripting	
Overview	13-1
Considerations	13-1
CLI Examples	13-1
Example #1: script	13-2

Example #2: script list and script delete	13-2
Example #3: script apply running-config.scr	13-2
Example #4: Creating a Configuration Script	13-3
Example #5: Upload a Configuration Script	13-3
Chapter 14	
Outbound Telnet	
Overview	14-1
CLI Examples	14-1
Example #1: show network	14-2
Example #2: show telnet	14-2
Example #3: transport output telnet	14-3
Example #4: session-limit and session-timeout	14-3
Chapter 15 Port Mirroring	
Overview	15-1
CLI Examples	15-1
Example #1: show monitor session	15-2
Example #2: show port all	15-2
Example #3: show port interface	15-2
Example #4: (Config) monitor session 1 mode	15-3
Example #5: (Config) monitor session 1 source interface	15-4
Example #6: (Interface) port security	15-4
Chapter 16	
Simple Network Time Protocol (SNTP)	
Overview	16-1
CLI Examples	16-1
Example #1: show sntp	16-1
Example #2: show sntp client	16-2
Example #3: show sntp server	16-2
Example #4: Configure SNTP	16-2
Chapter 17	
Pre-Login Banner	
Overview	17-1
CLI Example	17-1

Chapter 18

Syslog

Overview	18-1
Persistent Log Files	18-1
Interpreting Log Files	18-2
CLI Examples	18-2
Example #1: show logging	18-3
Example #2: show logging buffered	18-3
Example #3: show logging traplogs	18-4
Example 4: show logging hosts	18-4
Example #5: logging port configuration	18-5

About This Book

This document provides an understanding of the CLI and Web configuration options for software Release 4.3 features.

Document Organization

This document provides examples of the use of the switch software in a typical network. It describes the use and advantages of specific functions provided by the 7000 Series Managed Switch, and includes information on configuring those functions using the Command Line Interface and Web Interface.

The switch software can operate as a Layer 2 switch, a Layer 3 router or a combination switch/router. The switch also includes support for network management and Quality of Service functions such as Access Control Lists and Differentiated Services. Which functions you choose to activate will depend on the size and complexity of your network: this document describes configuration for some of the most-used functions.

This document contains configuration information about the following:

- Layer 2
 - VLANs
 - Routing
- Layer 3
 - Port routing
 - VLAN Routing
 - Virtual Router Redundancy Protocol (VRRP)
 - RIP
 - OSPF
 - Proxy ARP
- Quality of Service (QoS)
 - Access Control Lists (ACLs)
 - Class of Service (CoS)
 - Differentiated Services

- Multicast
 - IGMP Snooping
- Security
 - Denial of Service
 - Port Security
- Operating System
 - Dual Configuration
- Tools
 - Alarm Manager
 - Traceroute
 - Configuration Scripting
 - Advance Keying
 - Prelogin Banner
 - Port Mirroring
 - SNTP
 - Syslog
 - Data Migration

Audience

Use this guide if you are a(n):

- Experienced system administrator who is responsible for configuring and operating a network using switch software
- Level 1 and Level 2 Support provider

To obtain the greatest benefit from this guide, you should have an understanding of the switch software base and should have read the specification for your networking device platform. You should also have a basic knowledge of Ethernet and networking concepts.

CLI Documentation

The *Command Line Reference* provides information about the CLI commands used to configure the switch and the stack. The document provides CLI descriptions, syntax, and default values.

Refer to the *Command Line Reference* for information for the command structure

Related Documentation

Before proceeding, read the Release Notes for this switch product. The Release Notes detail the platform specific functionality of the Switching, Routing, SNMP, Config, Management, and other packages.

- Extending the portfolio of supported switching silicon to the broadest range in the industry
- Increasing the software's Quality of Service and Class of Service capabilities with integrated Layer 2, 3, and 4 Access Control Lists
- Improving switch's industry-leading Switching package with new features in the areas of IGMP, port mirroring, and others

Chapter 1

Getting Started

Connect a terminal to the switch to begin configuration.

In-band and Out-of-band Connectivity

Ask the system administrator to determine whether you will configure the switch for in-band or out-of-band connectivity.

Configuring for In-band Connectivity

In-band connectivity allows you to access the switch from a remote workstation using the Ethernet network. To use in-band connectivity, you must configure the switch with IP information (IP address, subnet mask, and default gateway).

Configure for In-band connectivity using one of the following methods:

- BootP or DHCP
- EIA-232 port

Using BootP or DHCP

You can assign IP information initially over the network or over the Ethernet service port through BootP or DHCP. Check with your system administrator to determine whether BootP or DHCP is enabled.

You need to configure the BootP or DHCP server with information about the switch —obtain this information through the serial port connection using the **show network** command. Set up the server with the following values:

IP Address	Unique IP address for the switch. Each IP parameter is made up of four decimal numbers, ranging from 0 to 255. The default for all IP parameters is zeroes (0.0.0.0).
Subnet	Subnet mask for the LAN
gateway	IP address of the default router, if the switch is a node outside the IP range of the LAN

MAC Address MAC address of the switch

When you connect the switch to the network for the first time after setting up the BootP or DHCP server, it is configured with the information supplied above. The switch is ready for in-band connectivity over the network.

If you do not use BootP or DHCP, access the switch through the EIA-232 port, and configure the network information as described below.

Using the EIA-232 Port

You can use a locally or remotely attached terminal to configure in-band management through the EIA-232 port.

1. To use a locally attached terminal, attach one end of a null-modem serial cable to the EIA-232 port of the switch and the other end to the COM port of the terminal or workstation. For remote attachment, attach one end of the serial cable to the EIA-232 port of the switch and the other end to the modem.
2. Set up the terminal for VT100 terminal emulation.
 - a. Set the terminal ON.
 - b. Launch the VT100 application.
 - c. Configure the COM port as follows:
 - Set the data rate to 115,200 baud.
 - Set the data format to 8 data bits, 1 stop bit, and no parity.
 - Set the flow control to none.
 - Select the proper mode under **Properties**.
 - Select Terminal keys.
3. The Log-in User prompt displays when the terminal interface initializes.

Enter an approved user name and password. The default is *admin* for the user name and the *password* is blank.

The switch is installed and loaded with the default configuration.

4. Reduce network traffic by turning off the Network Configuration Protocol. Enter the following command:

```
configure network protocol none
```

5. Set the IP address, subnet mask, and gateway address by issue the following command:


```
config network parms ipaddress netmask gateway
```

IP Address Unique IP address for the switch. Each IP parameter is made up of four decimal numbers, ranging from 0 to 255. The default for all IP parameters is zeroes (0.0.0.0).

Subnet Subnet mask for the LAN.

gateway IP address of the default router, if the switch is a node outside the IP range of the LAN.

6. To enable these changes to be retained during a reset of the switch, type **Ctrl-Z** to return to the main prompt, type **save config** at the main menu prompt, and type **y** to confirm the changes.
7. To view the changes and verify in-band information, issue the command: **show network**.
8. The switch is configured for in-band connectivity and ready for Web-based management.

Configuring for Out-Of-Band Connectivity

To monitor and configure the switch using out-of-band connectivity, use the console port to connect the switch to a terminal desktop system running terminal emulation software. The console port connector is a male DB-9 connector, implemented as a data terminal equipment (DTE) connector.

The following hardware is required to use the console port:

- VT100-compatible terminal, or a desktop, or a portable system with a serial port running VT100 terminal emulation software.
- An RS-232 crossover cable with a female DB-9 connector for the console port and the appropriate connector for the terminal.

Perform the following tasks to connect a terminal to the switch console port using out-of-band connectivity:

1. Connect an RS-232 crossover cable to the terminal running VT100 terminal emulation software.
2. Configure the terminal emulation software as follows:
 - a. Select the appropriate serial port (serial port 1 or serial port 2) to connect to the console.
 - b. Set the data rate to 115,200 baud.
 - c. Set the data format to 8 data bits, 1 stop bit, and no parity.
 - d. Set the flow control to none.

- e. Select the proper mode under **Properties**.
- f. Select Terminal keys.



Note: When using HyperTerminal with Microsoft Windows 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. With Windows 2000 Service Pack 2, the arrow keys function properly in HyperTerminal's VT100 emulation. Go to www.microsoft.com for more information on Windows 2000 service packs.

3. Connect the female connector of the RS-232 crossover cable directly to the switch console port, and tighten the captive retaining screws.

Starting the Switch

1. Make sure that the switch console port is connected to a VT100 terminal or VT100 terminal emulator via the RS-232 crossover cable.
2. Locate an AC power receptacle.
3. Deactivate the AC power receptacle.
4. Connect the switch to the AC receptacle.
5. Activate the AC power receptacle.

When the power is turned on with the local terminal already connected, the switch goes through a power-on self-test (POST). POST runs every time the switch is initialized and checks hardware components to determine if the switch is fully operational before completely booting. If POST detects a critical problem, the startup procedure stops. If POST passes successfully, a valid executable image is loaded into RAM. POST messages are displayed on the terminal and indicate test success or failure. The boot process runs for approximately 60 seconds.

Initial Configuration

The initial simple configuration procedure is based on the following assumptions:

- The switch was not configured before and is in the same state as when you received it.
- The switch booted successfully.

- The console connection was established and the console prompt appears on the screen of a VT100 terminal or terminal equivalent.

The initial switch configuration is performed through the console port. After the initial configuration, you can manage the switch either from the already-connected console port or remotely through an interface defined during the initial configuration.

The switch is not configured with a default user name and password.

All of the settings below are necessary to allow the remote management of the switch through Telnet (Telnet client) or HTTP (Web browser).

Before setting up the initial configuration of the switch, obtain the following information from your network administrator:

- The IP address to be assigned to the management interface through which the switch is managed.
- The IP subnet mask for the network.
- The IP address of the default gateway.

Initial Configuration Procedure

You can perform the initial configuration using the Easy Setup Wizard or by using the Command Line Interface (CLI). The Setup Wizard automatically starts when the switch configuration file is empty. You can exit the wizard at any point by entering [ctrl+z]. For more information on CLI initial configuration, see the *User's Configuration Guide*. This guide shows how to use the Setup Wizard for initial switch configuration. The wizard sets up the following configuration on the switch:

- Establishes the initial privileged user account with a valid password. The wizard configures one privileged user account during the set up.
- Enables CLI login and HTTP access to use the local authentication setting only.
- Sets up the IP address for the management interface.
- Sets up the SNMP community string to be used by the SNMP manager at a given IP address. You may choose to skip this step if SNMP management is not used for this switch.
- Allows you to specify the management server IP or permit SNMP access from all IP addresses.
- Configures the default gateway IP address.

Software Installation

This section contains procedures to help you become acquainted quickly with the switch software.

Before installing switch software, you should verify that the switch operates with the most recent firmware.

Quick Starting the Networking Device

1. Configure the switch for In-band or Out-of-Band connectivity. In-band connectivity allows access to the software locally or from a remote workstation. You must configure the device with IP information (IP address, subnet mask, and default gateway).
2. Turn the Power ON.
3. Allow the device to load the software until the login prompt appears. The device initial state is called the default mode.
4. When the prompt asks for operator login, do the following steps:
 - Type **admin** at the login prompt. Since a number of the Quick Setup commands require administrator account rights, log in to an administrator account.
 - Do not enter a password because the default mode does not use a password.
 - Check the CLI User EXEC prompt is displayed.
 - Enter **enable** to switch to the Privileged EXEC mode from User EXEC.
 - Enter **configure** to switch to the Global Config mode from Privileged EXEC.
 - Enter **exit** to return to the previous mode.
 - Enter **?** to show a list of commands that are available in the current mode.

System Information and System Setup

This section describes the commands you use to view system information and to setup the network device. Table 1-1 contains the Quick Start commands that allow you to view or configure the following information:

- Software versions
- Physical port data
- User account management
- IP address configuration

- Uploading from Networking Device to Out-of-Band PC (Only XMODEM)
- Downloading from Out-of-Band PC to Networking Device (Only XMODEM)
- Downloading from TFTP Server
- Restoring factory defaults

If you configure any network parameters, you should execute the following command:

```
copy system:running-config nvram:startup-config
```

This command saves the changes to the configuration file. You must be in the correct mode to execute the command. If you do not save the configuration, all changes are lost when a you power down or reset the networking device. In a stacking environment, the running configuration is saved in all units of the stack.

Table 1-1 describes the command syntax, the mode you must be in to execute the command, and the purpose and output of the command.

Table 1-1. Quick Start Commands

Command	Mode	Description
show hardware	Privileged EXEC	Shows hardware version, MAC address, and software version information.
show users	Privileged EXEC	Displays all of the users that are allowed to access the networking device. Access Mode shows whether you can change parameters on the networking device (Read/Write) or can only view them (Read Only). As a factory default, the 'admin' user has Read/Write access and the 'guest' user has Read Only access. There can only be one Read/Write user. There can be up to five Read Only users.
show login session	User EXEC	Displays all of the login session information.
users passwd <username>	Global Config	Allows the user to set passwords or change passwords needed to login. A prompt appears after the command is entered requesting the users old password. In the absence of an old password leave the area blank. User password should not be more than eight characters in length.

Table 1-1. Quick Start Commands

Command	Mode	Description
<code>copy system:running-config nvram:startup-config</code>	Privileged EXEC	Saves passwords and all other changes to the device. If you do not save the configuration, all changes are lost when you power down or reset the networking device. In a stacking environment, the running configuration is saved in all units of the stack.
<code>logout</code>	User EXEC Privileged EXEC	Logs the user out of the networking device.
<code>show network</code>	User EXEC	Displays the following network configuration information: <ul style="list-style-type: none"> • IP Address - IP Address of the interface (default: 0.0.0.0) • Subnet Mask - IP Subnet Mask for the interface (default: 0.0.0.0) • Default Gateway - The default Gateway for this interface (default: 0.0.0.0) • Burned in MAC Address - The Burned in MAC Address used for in-band connectivity • Locally Administered MAC Address - Can be configured to allow a locally administered MAC address • MAC Address Type - Specifies which MAC address should be used for in-band connectivity • Network Configurations Protocol Current - Indicates which network protocol is being used (default: none) • Management VLAN Id - Specifies VLAN id • Web Mode - Indicates whether HTTP/Web is enabled. • Java Mode - Indicates whether java mode is enabled.
<code>network parms</code> <code><ipaddr> <net-mask> [gateway]</code>	Privileged EXEC	Sets the IP address, subnet mask and gateway of the router. The IP address and the gateway must be on the same subnet. IP address range is from 0.0.0.0 to 255.255.255.255.
<code>copy nvram:startup-config</code> <code><tftp://<ipaddress>/<file-path>/<filename>></code>	Privileged EXEC	Starts the configuration file upload, displays the mode and type of upload and confirms the upload is progressing. The URL must be specified as: xmodem:<filepath>/<filename> For example: If the user is using HyperTerminal, the user must specify where the file is going to be received by the PC.

Table 1-1. Quick Start Commands

Command	Mode	Description
copy nvram:error-log <tftp://<ipaddress>/<filepath>/<filename>>	Privileged EXEC	Starts the error log upload, displays the mode and type of upload and confirms the upload is progressing. The URL must be specified as: xmodem:<filepath>/<filename>
copy nvram:traplog <tftp://<ipaddress>/<filepath>/<filename>>	Privileged EXEC	Starts the trap log upload, displays the mode and type of upload and confirms the upload is progressing. The URL must be specified as: xmodem:<filepath>/<filename>
copy <tftp://<ipaddress>/<filepath>/<filename>> nvram:startup-config	Privileged EXEC	Sets the destination (download) datatype to be an image (system:image) or a configuration file (nvram:startup-config). The URL must be specified as: xmodem:<filepath>/<filename> For example: If the user is using Hyper Terminal, the user must specify which file is to be sent to the networking device. The Networking Device restarts automatically once the code has been downloaded.
copy <tftp://<ipaddress>/<filepath>/<filename>> system:image	Privileged EXEC	Sets the destination (download) datatype to be an image (system:image) or a configuration file (nvram:startup-config). The URL must be specified as: xmodem:<filepath>/<filename>
copy <tftp://<ipaddress>/<filepath>/<filename>> nvram:startup-config	Privileged EXEC	Sets the destination (download) datatype to be a configuration file. The URL must be specified as: tftp://<ipaddress>/<filepath>/<filename> Before starting a TFTP server download, you must configure the IP address.

Table 1-1. Quick Start Commands

Command	Mode	Description
<code>copy <tftp:// <ipaddress>/ <filepath>/<file- name>> sys- tem:image</code>	Privileged EXEC	Sets the destination (download) datatype to be an image. The URL must be specified as: tftp://<ipaddress>/<filepath>/<filename> The system:image option downloads the code file.
<code>clear config</code>	Privileged EXEC	Enter yes when the prompt asks if you want to clear all the configurations made to the networking device.
<code>copy system:run- ning-config nvram:startup- config</code>	Privileged EXEC	Enter yes when the prompt asks if you want to save the configurations made to the networking device.
<code>reload</code> (or cold boot the networking device)	Privileged EXEC	Enter yes when the prompt asks if you want to reset the system. You can reset the networking device or cold boot the networking device. Both work effectively.

Chapter 2

Using the Web Interface

This chapter is a brief introduction to the web interface — it explains how to access the Web-based management panels to configure and manage the system.



Tip: Use the Web interface for configuration instead of the CLI interface. Web configuration is quicker and easier than entering the multiple required CLI commands. There are equivalent functions in the Web interface and the terminal interface—that is, both applications usually employ the same menus to accomplish a task. For example, when you log in, there is a Main Menu with the same functions available.

You can manage your switch through a Web browser and Internet connection. This is referred to as Web-based management. To use Web-based management, the system must be set up for in-band connectivity.

To access the switch, the Web browser must support:

- HTML version 4.0, or later
- HTTP version 1.1, or later
- JavaScript^(TM) version 1.2, or later

There are several differences between the Web and terminal interfaces. For example, on the Web interface the entire forwarding database can be displayed, while the terminal interface only displays 10 entries starting at specified addresses.

To terminate the Web login session, close the web browser.

Configuring for Web Access

To enable Web access to the switch:

1. Configure the switch for in-band connectivity. The switch *Getting Started Guide* provides instructions.
2. Enable Web mode:

- a. At the CLI prompt, enter the **show network** command.
- b. Set **Web Mode** to Enabled.

Starting the Web Interface

Follow these steps to start the switch Web interface:

1. Enter the IP address of the switch in the Web browser address field.
2. When the Login panel is displayed click **Login**.
3. Enter the appropriate User Name and Password. The User Name and associated Password are the same as those used for the terminal interface. Click on the Login button.
4. The System Description Menu displays, with the navigation tree appearing to the left of the screen.
5. Make a selection by clicking on the appropriate item in the navigation tree.

Web Page Layout

A Web interface panel for the switch Web page consists of three areas.

A banner graphic of the switch appears across the top of the panel.

The second area, a hierarchical-tree view appears to the left of the panel. The tree consists of a combination of folders, subfolders, and configuration and status HTML pages. You can think of the folders and subfolders as branches and the configuration and status HTML pages as leafs. Only the selection of a leaf (not a folder or subfolder) will cause the display of a new HTML page. A folder or subfolder has no corresponding HTML page.

The third area, at the bottom-right of the panel, displays the currently selected device configuration status and/or the user configurable information that you have selected from the tree view.

Configuring an SNMP V3 User Profile

Configuring an SNMP V3 user profile is a part of user configuration. Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, additional steps are needed. Use the following steps to configure an SNMP V3 new user profile.

1. Select **System>Configuration>User Accounts** from the hierarchical tree on the left side of the web interface.
2. Using the **User** pulldown menu, select **Create** to create a new user.

3. Enter a new user name in the User Name field.
4. Enter a new user password in the Password field and then retype it in the Confirm Password field.



Note: If SNMPv3 Authentication is to be used for this user, the password must be eight or more alphanumeric characters.

5. If you do not need authentication, go to Step 9.
6. To enable authentication, use the **Authentication Protocol** pulldown menu to select either MD5 or SHA for the authentication protocol.
7. If you do not need encryption, go to Step 9.
8. To enable encryption, use the **Encryption Protocol** pulldown menu to select **DES** for the encryption scheme. Then, enter in the Encryption Key field an encryption code of eight or more alphanumeric characters.
9. Click **Submit**.

Command Buttons

The following command buttons are used throughout the Web interface panels for the switch:

Save	Pressing the Save button implements and saves the changes you just made. Some settings may require you to reset the system in order for them to take effect.
Refresh	Pressing the Refresh button that appears next to the Apply button in Web interface panels refreshes the data on the panel.
Submit	Pressing the Submit button sends the updated configuration to the switch. Configuration changes take effect immediately, but these changes are not retained across a power cycle unless a save is performed.

Chapter 3

Virtual LANs

Adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. You may have many reasons for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

The Private Edge VLAN feature lets you set protection between ports located on the switch. This means that a protected port cannot forward traffic to another protected port on the same switch.

The feature does not provide protection between ports located on different switches.

VLAN Configuration Example

The diagram in this section shows a switch with four ports configured to handle the traffic for two VLANs. port 1/0/2 handles traffic for both VLANs, while port 1/0/1 is a member of VLAN 2 only, and ports 1/0/3 and 1/0/4 are members of VLAN 3 only. The script following the diagram shows the commands you would use to configure the switch as shown in the diagram.

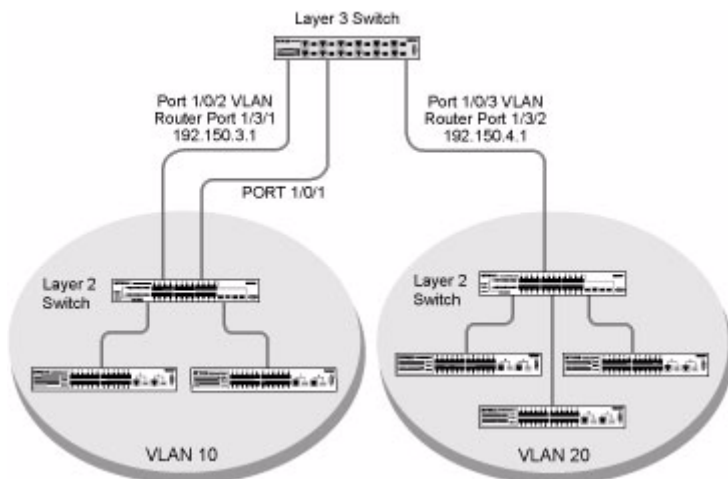


Figure 3-1

CLI Examples

The following examples show how to create VLANs, assign ports to the VLANs, and assign a VLAN as the default VLAN to a port.

Example #1: Create Two VLANs

Use the following commands to create two VLANs and to assign the VLAN IDs while leaving the names blank.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2
(Netgear Switch) (Vlan)#vlan 3
(Netgear Switch) (Vlan)#exit
```

Example #2: Assign Ports to VLAN2

This sequence shows how to assign ports to VLAN2, specify that frames will always be transmitted tagged from all member ports, and that untagged frames will be rejected on receipt.

```
(Netgear Switch) # config
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan acceptframe vlanonly
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan pvid 2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#exit
(Netgear Switch) (Config)#vlan port tagging all 2
(Netgear Switch) (Config)#
```

Example #3: Assign Ports to VLAN3

This example shows how to assign the ports that will belong to VLAN 3, and to specify that untagged frames will be accepted on port 1/0/4.

Note that port 1/0/2 belongs to both VLANs and that port 1/0/1 can never belong to VLAN 3.

```
(Netgear Switch) (Config)#interface range 1/0/2-1/0/4
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#vlan participation include 3
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#vlan acceptframe all
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

Example #4: Assign VLAN3 as the Default VLAN

This example shows how to assign VLAN 3 as the default VLAN for port 1/0/2.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan pvid 3
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Graphical User Interface

Use the following screens to perform the same configuration using the Graphical User Interface:

- **Switching --> VLAN--> Configuration.** To create the VLANs and specify port participation.
- **Switching --> VLAN --> Port Configuration.** To specify the handling of untagged frames on receipt, and whether frames will be transmitted tagged or untagged.

Chapter 4 Link Aggregation

This section includes instructions on configuring Link Aggregation using the Command Line Interface and the Graphical User Interface.

Link Aggregation (LAG) allows the switch to treat multiple physical links between two end-points as a single logical link. All of the physical links in a given LAG must operate in full-duplex mode at the same speed.

Link Aggregation can be used to directly connect two switches when the traffic between them requires high bandwidth and reliability, or to provide a higher bandwidth connection to a public network. LAG offers the following benefits:

- Increased reliability and availability -- if one of the physical links in the LAG goes down, traffic is dynamically and transparently reassigned to one of the other physical links.
- Better use of physical resources -- traffic can be load-balanced across the physical links.
- Increased bandwidth -- the aggregated physical links deliver higher bandwidth than each individual link.
- Incremental increase in bandwidth -- A physical upgrade could produce a 10-times increase in bandwidth; LAG produces a two- or five-times increase, useful if only a small increase is needed.

Management functions treat a LAG as if it were a single physical port.

You can include a LAG in a VLAN. You can configure more than one LAG for a given switch.

CLI Example

This section provides an example of configuring the software to support Link Aggregation (LAG) to a server and to a Layer 3 switch.

Figure 4-1 shows the example network.

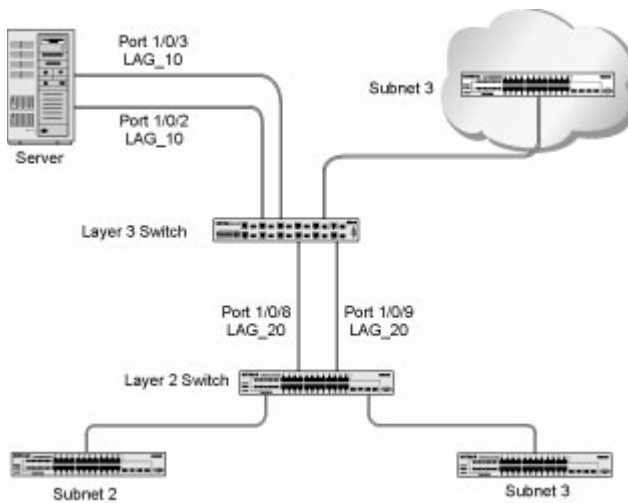


Figure 4-1

Example 1: Create two LAGS:

```
(Netgear Switch) #config
(Netgear Switch) (Config)#port-channel lag_10
(Netgear Switch) (Config)#port-channel lag_20
(Netgear Switch) (Config)#exit
```

Use the **show port-channel all** command to show the logical interface ids you will use to identify the LAGs in subsequent commands. Assume that lag_10 is assigned id 1/1/1 and lag_20 is assigned id 1/1/2.

```
(Console) #show port-channel all
```

Log. Intf	Port- Channel Name	Link Link	Adm. Mode	Trap Mode	STP Mode	Mbr Type	Ports	Port Speed	Port Active
1/1/1	lag_10	Down	En.	En.	Dis.	Dynamic			
1/1/2	lag_20	Down	En.	En.	Dis.	Dynamic			

Example 2: Add the ports to the LAGs:

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/2
(Netgear Switch) (Interface 0/2)#addport 1/1
(Netgear Switch) (Interface 0/2)#exit
(Netgear Switch) (Config)#interface 0/3
(Netgear Switch) (Interface 0/3)#addport 1/1
(Netgear Switch) (Interface 0/3)#exit
(Netgear Switch) (Config)#interface 0/8
(Netgear Switch) (Interface 0/8)#addport 1/2
(Netgear Switch) (Interface 0/8)#exit
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#addport 1/2
(Netgear Switch) (Interface 0/9)#exit
(Netgear Switch) (Config)#exit
```

Example 3: Enable both LAGs.

By default, the system enables link trap notification

```
(Console) #config
(Console) (Config)#port-channel adminmode all
(Console) (Config)#exit
```

At this point, the LAGs could be added to VLANs.

Chapter 5

IP Routing Services

IP routing services are divided into five areas:

- Port Routing
- VLAN Routing
- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF) Protocol
- Proxy Address Resolution Protocol (ARP)

Port Routing

The first networks were small enough for the end stations to communicate directly. As networks grew, Layer 2 bridging was used to segregate traffic, a technology that worked well for unicast traffic, but had problems coping with large quantities of multicast packets. The next major development was routing, where packets were examined and redirected at Layer 3. End stations needed to know how to reach their nearest router, and the routers had to understand the network topology so that they could forward traffic. Although bridges tended to be faster than routers, using routers allowed the network to be partitioned into logical subnetworks, which restricted multicast traffic and also facilitated the development of security mechanisms.

An end station specifies the destination station's Layer 3 address in the packet's IP header, but sends the packet to the MAC address of a router. When the Layer 3 router receives the packet, it will minimally:

- Look up the Layer 3 address in its address table to determine the outbound port
- Update the Layer 3 header
- Recreate the Layer 2 header

The router's IP address is often statically configured in the end station, although the 7000 Series Managed Switch supports protocols such as DHCP that allow the address to be assigned dynamically. Likewise, you may assign some of the entries in the routing tables used by the router statically, but protocols such as RIP and OSPF allow the tables to be created and updated dynamically as the network configuration changes.

Port Routing Configuration

The 7000 Series Managed Switch always supports Layer 2 bridging, but Layer 3 routing must be explicitly enabled, first for the 7000 Series Managed Switch as a whole, and then for each port which is to participate in the routed network.

The configuration commands used in the example in this section enable IP routing on ports 1/0/2, 1/0/3, and 1/0/5. The router ID will be set to the 7000 Series Managed Switch's management IP address, or to that of any active router interface if the management address is not configured.

After the routing configuration commands have been issued, the following functions will be active:

- IP Forwarding, responsible for forwarding received IP packets.
- ARP Mapping, responsible for maintaining the ARP Table used to correlate IP and MAC addresses. The table contains both static entries and entries dynamically updated based on information in received ARP frames.
- Routing Table Object, responsible for maintaining the common routing table used by all registered routing protocols.

You may then activate RIP or OSPF, used by routers to exchange route information, on top of IP Routing. RIP is more often used in smaller networks, while OSPF was designed for larger and more complex topologies.

CLI Examples

This diagram shows a Layer 3 switch configured for port routing. It connects three different subnets, each connected to a different port. The script shows the commands you would use to configure a 7000 Series Managed Switch to provide the port routing support shown in the diagram.

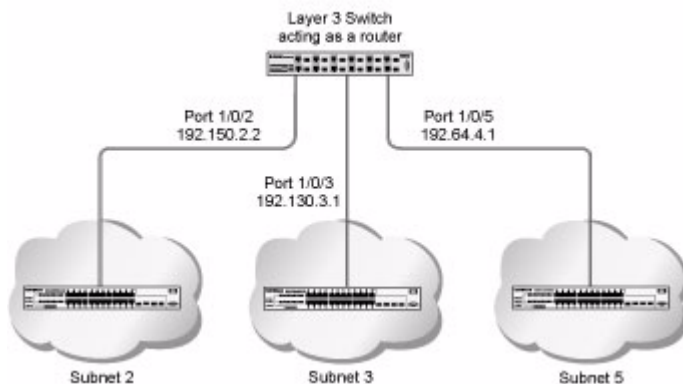


Figure 5-1

Example 1. Enabling routing for the Switch

Use the following command to enable routing for the switch. Execution of the command enables IP forwarding by default.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

Example 2. Enabling Routing for Ports on the Switch

Use the following commands to enable routing for ports on the switch. The default link-level encapsulation format is Ethernet. Configure the IP addresses and subnet masks for the ports. Network directed broadcast frames will be dropped and the maximum transmission unit (MTU) size will be 1500 bytes.

```
(Netgear Switch) #config
(Netgear Switch) (Config)# interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit

(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)# routing
(Netgear Switch) (Interface 1/0/5)#ip address 192.150.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Config)#exit
```

VLAN Routing

You can configure 7000 Series Managed Switch with some ports supporting VLANs and some supporting routing. You can also configure it to allow traffic on a VLAN to be treated as if the VLAN were a router port.

When a port is enabled for bridging (the default) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its MAC Destination Address (DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet will be routed. An inbound multicast packet will be forwarded to all ports in the VLAN, plus the internal bridge-router interface if it was received on a routed VLAN.

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN Routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required.

The next section will show you how to configure the 7000 Series Managed Switch to support VLAN routing and how to use RIP and OSPF. A port may be either a VLAN port or a router port, but not both. However, a VLAN port may be part of a VLAN that is itself a router port.

VLAN Routing Configuration

This section provides an example of how to configure 7000 Series Managed Switch to support VLAN routing. The configuration of the VLAN router port is similar to that of a physical port. The main difference is that, after the VLAN has been created, you must use the **show ip vlan** command to determine the VLAN's interface ID so that you can use it in the router configuration commands.

CLI Examples

The diagram in this section shows a Layer 3 switch configured for port routing. It connects two VLANs, with two ports participating in one VLAN, and one port in the other. The script shows the commands you would use to configure a 7000 Series Managed Switch to provide the VLAN routing support shown in the diagram.

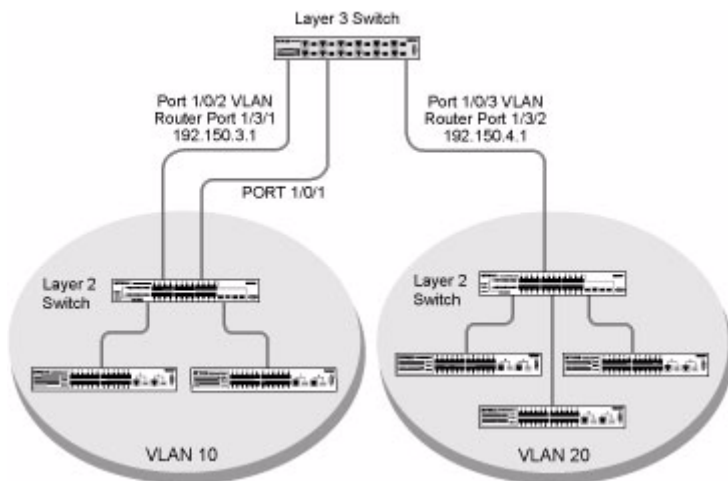


Figure 5-2

Example 1: Create Two VLANs

The following code sequence shows an example of creating two VLANs with egress frame tagging enabled.

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan pvid 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 20
(Netgear Switch) (Interface 1/0/3)#vlan pvid 20
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#vlan port tagging all 10
(Netgear Switch) (Config)#vlan port tagging all 20
(Netgear Switch) (Config)#exit
```

Example 2: Set Up VLAN Routing for the VLANs and the Switch.

The following code sequence shows how to enable routing for the VLANs:

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
```

This returns the logical interface IDs that will be used instead of slot/port in subsequent routing commands. Assume that VLAN 10 is assigned ID 3/1 and VLAN 20 is assigned ID 3/2.

Enable routing for the switch:

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

The next sequence shows an example of configuring the IP addresses and subnet masks for the virtual router ports.

```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface-vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface-vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface-vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface-vlan 20)#exit
(Netgear Switch) (Config)#exit
```

VLAN Routing RIP Configuration

Routing Information Protocol (RIP) is one of the protocols which may be used by routers to exchange network topology information. It is characterized as an “interior” gateway protocol, and is typically used in small to medium-sized networks.

A router running RIP will send the contents of its routing table to each of its adjacent routers every 30 seconds. When a route is removed from the routing table it will be flagged as unusable by the receiving routers after 180 seconds, and removed from their tables after an additional 120 seconds.

There are two versions of RIP:

- IPv1 defined in RFC 1058
 - Routes are specified by IP destination network and hop count
 - The routing table is broadcast to all stations on the attached network
- IPv2 defined in RFC 1723
 - Route specification is extended to include subnet mask and gateway
 - The routing table is sent to a multicast address, reducing network traffic
 - An authentication method is used for security

The 7000 Series Managed Switch supports both versions of RIP. You may configure a given port:

- To receive packets in either or both formats
- To transmit packets formatted for IPv1 or IPv2 or to send IPv2 packets to the IPv1 broadcast address
- To prevent any RIP packets from being received
- To prevent any RIP packets from being transmitted.

CLI Example

This example adds support for RIPv2 to the configuration created in the base VLAN routing example. A second router, using port routing rather than VLAN routing, has been added to the network.

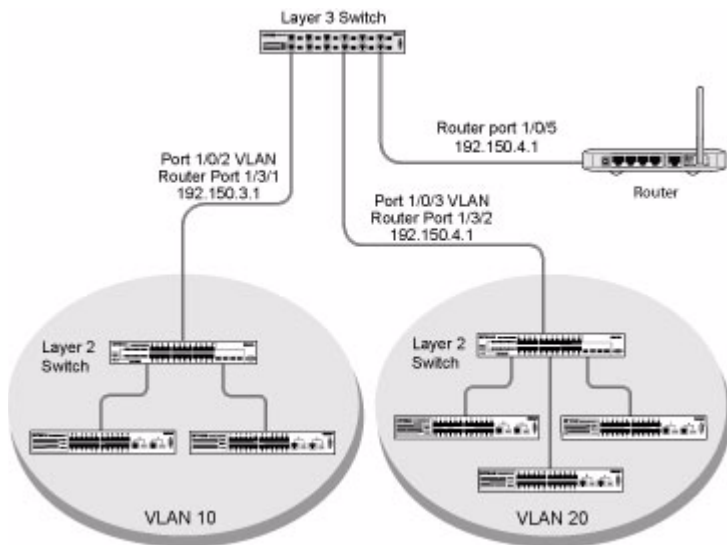


Figure 5-3

Example of configuring VLAN Routing with RIP support on a 7000 Series Managed Switch

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#vlan port tagging all 10
(Netgear Switch) (Config)#vlan port tagging all 20
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan participation include 10
(Netgear Switch) (Interface 1/0/2)#vlan pvid 10
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 20
(Netgear Switch) (Interface 1/0/3)#vlan pvid 20
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface vlan 20)#exit
```

Enable RIP for the switch. The route preference will default to 15.

```
(Netgear Switch) (Config)#router rip
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit
```

Configure the IP address and subnet mask for a non-virtual router port.

```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#ip address 192.150.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/5)#exit
```

Enable RIP for the VLAN router ports. Authentication will default to none, and no default route entry will be created.

```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip rip
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)# interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip rip
(Netgear Switch) (Interface vlan 20)#exit
(Netgear Switch) (Config)#exit
```

VLAN Routing OSPF Configuration

For larger networks Open Shortest Path First (OSPF) is generally used in preference to RIP. OSPF offers several benefits to the administrator of a large and/or complex network:

- Less network traffic:
 - Routing table updates are sent only when a change has occurred
 - Only the part of the table which has changed is sent
 - Updates are sent to a multicast, not a broadcast, address
- Hierarchical management, allowing the network to be subdivided

The top level of the hierarchy of an OSPF network is known as an autonomous system (AS) or routing domain, and is a collection of networks with a common administration and routing strategy. The AS is divided into areas: intra-area routing is used when a source and destination address are in the same area, and inter-area routing across an OSPF backbone is used when they are not. An inter-area router communicates with border routers in each of the areas to which it provides connectivity.

The 7000 Series Managed Switch operating as a router and running OSPF will determine the best route using the assigned cost and the type of the OSPF route. The order for choosing a route if more than one type of route exists is as follows:

- Intra-area
- Inter-area
- External type 1: the route is external to the AS
- External Type 2: the route was learned from other protocols such as RIP

CLI Example

This example adds support for OSPF to the configuration created in the base VLAN routing example. The script shows the commands you would use to configure the 7000 Series Managed Switch as an inter-area router. Refer to [Figure 5-2](#).

Example of configuring OSPF on a 7000 Series Managed Switch acting as an inter-area router:

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#vlan port tagging all 10
(Netgear Switch) (Config)#vlan port tagging all 20
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan participation include 10
(Netgear Switch) (Interface 1/0/2)#vlan pvid 10
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 20
(Netgear Switch) (Interface 1/0/3)#vlan pvid 20
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface vlan 20)#exit
```

Specify the router ID and enable OSPF for the switch.

```
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config router)#router-id 192.150.9.9
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit
```

Enable OSPF for the VLAN and physical router ports.

```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface vlan 10)#ip ospf
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)# ip ospf areaid 0.0.0.3
(Netgear Switch) (Interface vlan 20)#ip ospf
(Netgear Switch) (Interface vlan 20)#exit
```

Set the OSPF priority and cost for the VLAN and physical router ports.

```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip ospf priority 128
(Netgear Switch) (Interface vlan 10)#ip ospf cost 32
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip ospf priority 255
(Netgear Switch) (Interface vlan 20)#ip ospf cost 64
(Netgear Switch) (Interface vlan 20)#exit
(Netgear Switch) (Config)#exit
```

Routing Information Protocol

Routing Information Protocol (RIP) is one of the protocols which may be used by routers to exchange network topology information. It is characterized as an “interior” gateway protocol, and is typically used in small to medium-sized networks.

RIP Configuration

A router running RIP will send the contents of its routing table to each of its adjacent routers every 30 seconds. When a route is removed from the routing table it will be flagged as unusable by the receiving routers after 180 seconds, and removed from their tables after an additional 120 seconds.

There are two versions of RIP:

- RIPv1 defined in RFC 1058
 - Routes are specified by IP destination network and hop count
 - The routing table is broadcast to all stations on the attached network
- RIPv2 defined in RFC 1723
 - Route specification is extended to include subnet mask and gateway
 - The routing table is sent to a multicast address, reducing network traffic
 - An authentication method is used for security

The 7000 Series Managed Switch supports both versions of RIP. You may configure a given port:

- To receive packets in either or both formats
- To transmit packets formatted for RIPv1 or RIPv2 or to send RIPv2 packets to the RIPv1 broadcast address
- To prevent any RIP packets from being received

- To prevent any RIP packets from being transmitted

CLI Example

The configuration commands used in the following example enable RIP on ports 1/0/2 and 1/0/3 as shown in the network illustrated in [Figure 5-4](#)

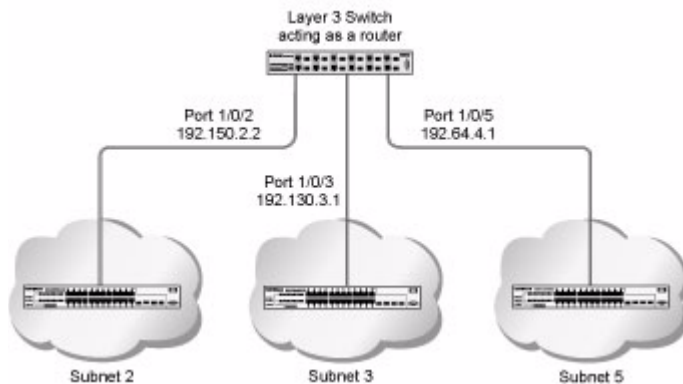


Figure 5-4

Example #1: Enable Routing for the Switch:

The following sequence enables routing for the switch:

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

Example #2: Enable Routing for Ports

The following command sequence enables routing and assigns IP addresses for ports 1/0/2 and 1/0/3.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

Example #3. Enable RIP for the Switch

The next sequence enables RIP for the switch. the route preference defaults to 15.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#router rip
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```

Example #4. Enable RIP for ports 1/0/2 and 1/0/3

This command sequence enables RIP for ports 1/0/2 and 1/0/3. Authentication defaults to none, and no default route entry is created. The commands specify that both ports receive both RIPv1 and RIPv2 frames, but send only RIPv2 formatted frames.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip rip
(Netgear Switch) (Interface 1/0/2)#ip rip receive version both
(Netgear Switch) (Interface 1/0/2)#ip rip send version rip2
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip rip
(Netgear Switch) (Interface 1/0/3)#ip rip receive version both
(Netgear Switch) (Interface 1/0/3)#ip rip send version rip2
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

OSPF

For larger networks Open Shortest Path First (OSPF) is generally used in preference to RIP. OSPF offers several benefits to the administrator of a large and/or complex network:

- Less network traffic:
 - Routing table updates are sent only when a change has occurred
 - Only the part of the table which has changed is sent
 - Updates are sent to a multicast, not a broadcast, address
- Hierarchical management, allowing the network to be subdivided

The top level of the hierarchy of an OSPF network is known as an autonomous system (AS) or routing domain, and is a collection of networks with a common administration and routing strategy. The AS is divided into areas: intra-area routing is used when a source and destination address are in the same area, and inter-area routing across an OSPF backbone is used when they are not. An inter-area router communicates with border routers in each of the areas to which it provides connectivity.

The 7000 Series Managed Switch operating as a router and running OSPF will determine the best route using the assigned cost and the type of the OSPF route. The order for choosing a route if more than one type of route exists is as follows:

- Intra-area
- Inter-area
- External type 1: the route is external to the AS
- External Type 2: the route was learned from other protocols such as RIP

CLI Examples

The examples in this section show you how to configure a 7000 Series Managed Switch first as an inter-area router and then as a border router. They show two areas, each with its own border router connected to one inter-area router.

The first diagram shows a network segment with an inter-area router connecting areas 0.0.0.2 and 0.0.0.3. The example script shows the commands used to configure a 7000 Series Managed Switch as the inter-area router in the diagram by enabling OSPF on port 1/0/2 in area 0.0.0.2 and port 1/0/3 in area 0.0.0.3.

Example #1 Configuring an Inter-Area Router

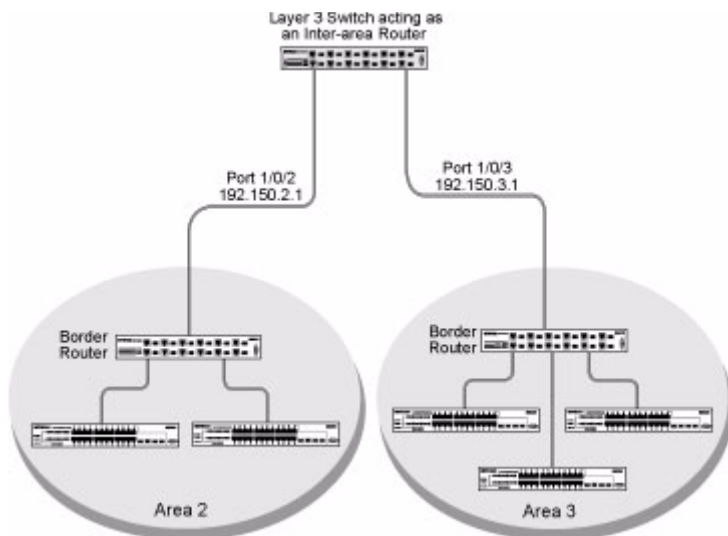


Figure 5-5

Enable Routing for the Switch. The following command sequence enables ip routing for the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

Assign IP Addresses for Ports. The following sequence enables routing and assigns IP addresses for ports 1/0/2 and 1/0/3:

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

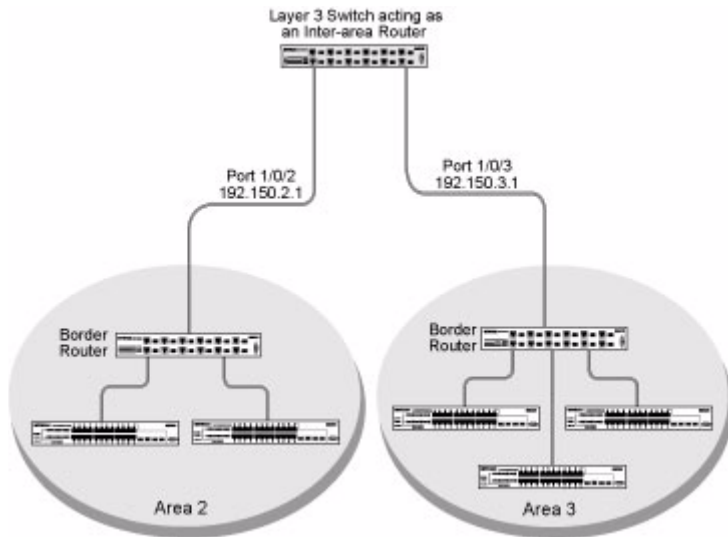
Specify Router ID and Enable OSPF for the Switch. The following sequence specifies the router ID and enables OSPF for the switch. Set disable1583 compatibility to prevent the routing loop.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#router-id 192.150.9.9
(Netgear Switch) (Config router)#no 1583compatibility
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```

Enable and Configure OSPF for the Ports. The following sequence enables OSPF and sets the OSPF priority and cost for the ports.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip ospf
(Netgear Switch) (Interface 1/0/2)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/2)#ip ospf priority 128
(Netgear Switch) (Interface 1/0/2)#ip ospf cost 32
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip ospf
(Netgear Switch) (Interface 1/0/3)#ip ospf areaid 0.0.0.3
(Netgear Switch) (Interface 1/0/3)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/3)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/3)#exit(Netgear Switch) (Config)#exit
```

Example #2 - Configuring OSPF on a Border Router**Figure 5-6**

The following example configures OSPF on a 7000 Series Managed Switch operating as a border router:

Enable routing for the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
```

Enable routing & assign IP for ports 1/0/2, 1/0/3 and 1/0/4.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.2 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.130.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#routing
(Netgear Switch) (Interface 1/0/4)#ip address 192.64.4.1 255.255.255.0
(Netgear Switch) (Interface 1/0/4)#exit
```

Specify the router ID and enable OSPF for the switch. Set disable 1583compatibility to prevent a routing loop.

```
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#router-id 192.130.1.1
(Netgear Switch) (Config router)#no 1583compatibility
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```


Enable OSPF for the ports and set the OSPF priority and cost for the ports.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip ospf
(Netgear Switch) (Interface 1/0/2)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/2)#ip ospf priority 128
(Netgear Switch) (Interface 1/0/2)#ip ospf cost 32
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip ospf
(Netgear Switch) (Interface 1/0/3)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/3)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/3)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/3)#exit

(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#ip ospf
(Netgear Switch) (Interface 1/0/4)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/4)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/4)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

Proxy Address Resolution Protocol (ARP)

This section describes the Proxy Address Resolution Protocol (ARP) feature.

Overview

- Proxy ARP allows a router to answer ARP requests where the target IP address is not the router itself but a destination that the router can reach
- If a host does not know the default gateway, proxy ARP can learn the first hop
- Machines in one physical network appear to be part of another logical network
- Without proxy ARP, a router will only respond to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived

CLI Examples

The following are examples of the commands used in the proxy ARP feature.

Example #1: show ip interface

```
(Netgear Switch) #show ip interface ?

<slot/port>          Enter an interface in slot/port format.
brief                Display summary information about IP configuration
                    settings for all ports.

(Netgear Switch) #show ip interface 0/24

Routing Mode..... Disable
Administrative Mode..... Enable
Forward Net Directed Broadcasts..... Disable
Proxy ARP..... Disable
Active State..... Inactive
Link Speed Data Rate..... Inactive
MAC Address..... 08:00:17:05:05:02
Encapsulation Type..... Ethernet
IP MTU..... 1500
```

Example #2: ip proxy-arp

```
(Netgear Switch) (Interface 0/24)#ip proxy-arp ?

<cr>                Press Enter to execute the command.

(Netgear Switch) (Interface 0/24)#ip proxy-arp
```

Chapter 6

Virtual Router Redundancy Protocol

When an end station is statically configured with the address of the router that will handle its routed traffic, a single point of failure is introduced into the network. If the router goes down, the end station is unable to communicate. Since static configuration is a convenient way to assign router addresses, Virtual Router Redundancy Protocol (VRRP) was developed to provide a backup mechanism.

VRRP eliminates the single point of failure associated with static default routes by enabling a backup router to take over from a “master” router without affecting the end stations using the route. The end stations will use a “virtual” IP address that will be recognized by the backup router if the master router fails. Participating routers use an election protocol to determine which router is the master router at any given time. A given port may appear as more than one virtual router to the network, also, more than one port on a 7000 Series Managed Switch may be configured as a virtual router. Either a physical port or a routed VLAN may participate.

CLI Examples

This example shows how to configure the 7000 Series Managed Switch to support VRRP. Router 1 will be the default master router for the virtual route, and Router 2 will be the backup router.

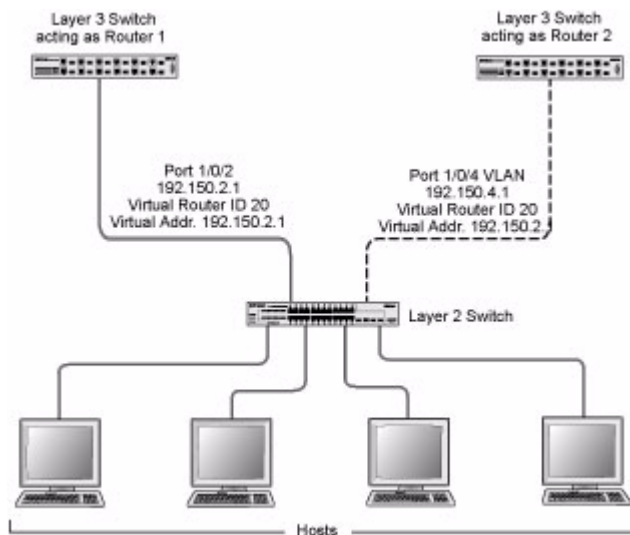


Figure 6-1

The following is an example of configuring VRRP on a 7000 Series Managed Switch acting as the master router:

```

    Enable routing for the switch. IP forwarding will then be enabled
    by default.
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing

    Configure the IP addresses and subnet masks for the port that will
    participate in the protocol.
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit

    Enable VRRP for the switch.
(Netgear Switch) (Config)#ip vrrp

    Assign virtual router IDs to the port that will participate in the
    protocol.
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20

    Specify the IP address that the virtual router function will rec-
    ognize. Note that the virtual IP address on port 1/0/2 is the same
    as the port's actual IP address, therefore this router will always
    be the VRRP master when it is active. And the priority default is
    255.
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20 ip 192.150.2.1

    Enable VRRP on the port.
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20 mode
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

The following is an example of configuring VRRP on a 7000 Series Managed Switch acting as the backup router:

```

    Enable routing for the switch. IP forwarding will then be enabled
    by default.
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing

    Configure the IP addresses and subnet masks for the port that will
    participate in the protocol.
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#routing
(Netgear Switch) (Interface 1/0/4)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface 1/0/4)#exit

    Enable VRRP for the switch.
(Netgear Switch) (Config)#ip vrrp 20

    Assign virtual router IDs to the port that will participate in the
    protocol.
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20

    Specify the IP address that the virtual router function will rec-
    ognize. Since the virtual IP address on port 1/0/4 is the same as
    Router 1's port 1/0/2 actual IP address, this router will always
    be the VRRP backup when Router 1 is active.
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 ip 192.150.2.1

    Set the priority for the port. The default priority is 100.
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 priority 254

    Enable VRRP on the port.
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 mode
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

Chapter 7

Access Control Lists (ACLs)

This section describes the Access Control Lists (ACLs) feature.

Overview

Access Control Lists (ACLs) can control the traffic entering a network. Normally ACLs reside in a firewall router or in a router connecting two internal networks. When you configure ACLs, you can selectively admit or reject inbound traffic, thereby controlling access to your network or to specific resources on your network.

You can set up ACLs to control traffic at Layer 2, or Layer3. MAC ACLs are used for Layer 2. IP ACLs are used for Layers 3.

Each ACL contains a set of rules that apply to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and may apply to one or more of the fields within a packet.

Limitations

The following limitations apply to ACLs. These limitations are platform dependent.

- Maximum of 100 ACLs
- Maximum rules per ACL is 8-10
- Stacking systems do not support redirection

The system does not support MAC ACLs and IP ACLs on the same interface.

The system supports ACLs set up for inbound traffic only.

MAC ACLs

MAC ACLs are Layer 2 ACLs. You can configure the rules to inspect the following fields of a packet (limited by platform):

- Source MAC address with mask

- Destination MAC address with mask
- VLAN ID (or range of IDs)
- Class of Service (CoS) (802.1p)
- Ethertype
- L2 ACLs can apply to one or more interfaces
- Multiple access lists can be applied to a single interface - sequence number determines the order of execution
- You cannot configure a MAC ACL and an IP ACL on the same interface
- You can assign packets to queues using the assign queue option
- You can redirect packets using the redirect option

Configuring IP ACLs

IP ACLs classify for Layer 3.

Each ACL is a set of up to ten rules applied to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and may apply to one or more of the following fields within a packet:

- Source IP address
- Destination IP address
- Source Layer 4 port
- Destination Layer 4 port
- TOS byte
- Protocol number

Note that the order of the rules is important: when a packet matches multiple rules, the first rule takes precedence. Also, once you define an ACL for a given port, all traffic not specifically permitted by the ACL will be denied access.

Process

To configure ACLs, follow these steps:

- Create an ACL by specifying a name (MAC ACL) or a number (IP ACL)
- Add new rules to the ACL
- Configure the match criteria for the rules
- Apply the ACL to one or more interfaces

IP ACL CLI Example

The script in this section shows you how to set up an IP ACL with two rules, one applicable to TCP traffic and one to UDP traffic. The content of the two rules is the same. TCP and UDP packets will only be accepted by the 7000 Series Managed Switch if the source and destination stations have IP addresses that fall within the defined sets.

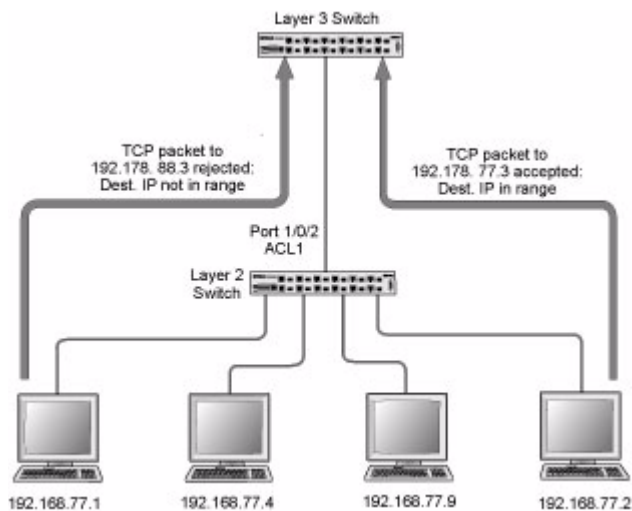


Figure 7-1

The following is an example of configuring ACL support on a 7000 Series Managed Switch:

```

        Create ACL 101.
        Define the first rule: it will permit packets with a match on the
        specified Source IP address, after the mask has been applied, that
        are carrying TCP traffic, and are sent to the specified
        Destination IP address.
(Netgear Switch) #config
(Netgear Switch) (Config)#access-list 101 permit tcp 192.168.77.0 0.0.0.255
192.178.77.0 0.0.0.255

        Define the second rule for ACL 101.
        Define the rule to set similar conditions for UDP traffic as for
        TCP traffic.
(Netgear Switch) (Config)#access-list 101 permit udp 192.168.77.0 0.0.0.255
192.178.77.0 0.0.0.255

        Apply the rule to inbound traffic on port 1/0/2. Only traffic
        matching the criteria will be accepted.
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip access-group 101 in
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

MAC ACL CLI Examples

The following are examples of the commands used for the MAC ACLs feature.

Example #1: mac access list

```
(Netgear Switch)(Config)#mac access-list ?  
  
extended      Configure extended MAC Access List parameters.  
  
Netgear Switch)(Config)#mac access-list extended ?  
  
<name>       Enter access-list name up to 31 characters in length.  
rename       Rename MAC Access Control List.  
  
(Netgear Switch) (Config)#mac access-list extended b1 ?  
  
<cr>        Press Enter to execute the command.  
  
(Netgear Switch) (Config)#mac access-list extended b1
```

Example #2: permit any

```
(Netgear Switch) (Config-mac access-list)#permit ?


```

Example #3 Configure mac access-group

```
(Netgear Switch) (Config)#interface 1/0/5

(Netgear Switch) (Interface 1/0/5)#mac ?

access-group      Attach MAC Access List to Interface.

(Netgear Switch) (Interface 1/0/5)#mac access-group ?

<name>           Enter name of MAC Access Control List.

(Netgear Switch) (Interface 1/0/5)#mac access-group b1 ?

in               Enter the direction <in>.

(Netgear Switch) (Interface 1/0/5)#mac access-group b1 in ?

<cr>             Press Enter to execute the command.

<1-4294967295>   Enter the sequence number (greater than 0) to rank precedence
                  for this interface and direction. A lower sequence number has
                  higher precedence.

(Netgear Switch) (Interface 1/0/5)#mac access-group b1 in
```

Example #4 permit

```
(Netgear Switch) (Config)#mac access-list extended b2

(Netgear Switch) (Config-mac-access-list)#permit 00:00:00:00:00:00 ?

<dstmac>      Enter a MAC Address.
any           Configure a a match condition for all the destination MAC
              addresses in the Destination MAC Address field.

(Netgear Switch) (Config-mac-access-list)#permit 00:00:00:00:00:00 any

access-queue   Configure the Queue Id assignment attribute.
cos           Configure a match condition based on a CoS value.
<ethertypekey> Enter one of the following keywords to specify an Ethertype
              (appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmlcast, mplsucast,
              netbios, novell, pppo,rarp).
<0x0600-0xffff> Enter a four-digit hexadecimal number in the range of 0x0600 to
              0xffff to specify a custom Ethertype value.
vlan          Configure a match condition based on a VLAN ID.
<cr>         Press Enter to execute the command.
```

Example #5: show mac access-lists

```
(Netgear Switch) #show mac access-lists
Current number of all ACLs: 2      Maximum number of all ACLs: 100

MAC ACL Name      Rules      Interface(s)      Direction
-----
b1                 1          1/0/5             inbound
b2                 1

(Netgear Switch)      #show mac access-lists ?

<name>      Enter access-list name up to 31 characters in length.
<cr>        Press Enter to execute the command.

(Netgear Switch)      #show mac access-lists b1 ?

<cr>        Press Enter to execute the command.

(Netgear Switch)      #show mac access-lists b1

Rule Number: 1
Action.....          permit
Match All.....       TRUE
```


Chapter 8

Class of Service (CoS) Queuing

This section describes the Class of Service (CoS) Queue Mapping and Traffic Shaping features.

Overview

Each port has one or more queues for packet transmission. During configuration, you can determine the mapping and configuration of these queues.

Based on service rate and other criteria you configure, queues provide preference to specified packets. If a delay becomes necessary, the system holds packets until the scheduler authorizes transmission. As queues become full, packets are dropped. Packet drop precedence indicates the packet's sensitivity to being dropped during times of queue congestion.

CoS mapping, queue parameters, and queue management are configurable per interface.

Queue management is configurable per interface.

Some hardware implementations allow queue depth management using tail dropping or Weighted random early discard (WRED).

Some hardware implementations allow queue depth management using tail dropping.

The operation of CoS Queuing involves queue mapping and queue configuration.

CoS Queue Mapping

CoS Queue Mapping uses trusted and untrusted ports.

Trusted Ports

- System takes at face value certain priority designation for arriving packets.
- Trust applies only to packets that have that trust information.
- Can only have one trust field at a time - per port.
 - 802.1p User Priority (default trust mode - Managed through Switching configuration)

- IP Precedence
- IP DiffServ Code Point (DSCP)

The system can assign service level based upon the 802.1p priority field of the L2 header. You configure this by mapping the 802.1p priorities to one of three traffic class queues. These queues are:

- Queue 2 - Minimum of 50% of available bandwidth
- Queue 1 - Minimum of 33% of available bandwidth
- Queue 0 - Lowest priority, minimum of 17% of available bandwidth

For untagged traffic, you can specify default 802.1p priority on a per-port basis.

Untrusted Ports

- No incoming packet priority designation is trusted, therefore the port default priority value is used.
- All ingress packets from Untrusted ports, where the packet is classified by an ACL or a DiffServ policy, are directed to specific CoS queues on the appropriate egress port. That specific CoS queue is determined by either the default priority of the port or a DiffServ or ACL assign queue attribute.
- Used when trusted port mapping is unable to be honored - i.e. when a non-IP DSCP packet arrives at a port configured to trust IP DSCP.

CoS Queue Configuration

CoS queue configuration involves port egress queue configuration and drop precedence configuration (per queue). The design of these on a per queue, per drop precedence basis allows the user to create the desired service characteristics for different types of traffic.

Port Egress Queue Configuration

- Scheduler Type
 - Strict vs. Weighted
- Minimum guaranteed bandwidth
- Maximum allowed bandwidth
 - Per queue shaping
- Queue management type

- Tail drop vs. WRED

Drop Precedence Configuration (per Queue)

- WRED parameters
 - Minimum threshold
 - Maximum threshold
 - Drop probability
 - Scale factor
- Tail Drop parameters
 - Threshold

Per Interface Basis

- Queue management type
 - Tail Drop vs. WRED

Only if per queue config is not supported

- WRED Decay Exponent
- Traffic Shaping
 - For an entire interface

CLI Examples

The following are examples of the commands used in the CoS Queuing feature.

Example #1: show classofservice trust

```
(Netgear Switch) #show classofservice trust ?  
  
<cr>                               Press Enter to execute the command.  
  
(Netgear Switch) #show classofservice trust  
  
Class of Service Trust Mode: Dot1P
```

Example #2: set classofservice trust mode

```
(Netgear Switch) (Config)#classofservice ?  
  
dot1p-mapping      Configure dot1p priority mapping.  
ip-dscp-mapping    Maps an IP DSCP value to an internal traffic class.  
trust              Sets the Class of Service Trust Mode of an Interface.  
  
(Netgear Switch) (Config)#classofservice trust ?  
  
dot1p              Sets the Class of Service Trust Mode of an Interface  
                   to 802.1p.  
ip-dscp            Sets the Class of Service Trust Mode of an Interface  
                   to IP DSCP.  
  
(Netgear Switch) (Config)#classofservice trust dot1p ?  
  
<cr>                               Press Enter to execute the command.  
  
(Netgear Switch) (Config)#classofservice trust dot1p
```

Example #3: show classofservice ip-precedence mapping

```
(Netgear Switch) #show classofservice ip-precedence-mapping
```

IP Precedence	Traffic Class
-----	-----
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Example #4: Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode

```
(Netgear Switch) (Config)#cos-queue min-bandwidth ?
```

```
<bw-0>                               Enter the minimum bandwidth percentage for Queue 0.
```

```
(Netgear Switch) (Config)#cos-queue min-bandwidth 15
```

```
Incorrect input! Use 'cos-queue min-bandwidth <bw-0>..<bw-7>.
```

```
(Netgear Switch) (Config)#cos-queue min-bandwidth 15 25 10 5 5 20 10 10
```

```
(Netgear Switch) (Config)#cos-queue strict ?
```

```
<queue-id>                           Enter a Queue Id from 0 to 7.
```

```
(Netgear Switch) (Config)#cos-queue strict 1 ?
```

```
<cr>                                  Press Enter to execute the command.
```

```
<queue-id>                           Enter an additional Queue Id from 0 to 7.
```

```
(Netgear Switch) (Config)#cos-queue strict 1
```

Example #5: Set CoS Trust Mode of an Interface

```
(Netgear Switch) (Config)#classofservice trust ?  
  
dot1p                Sets the Class of Service Trust Mode of an Interface  
                      to 802.1p.  
ip-dscp              Sets the Class of Service Trust Mode of an Interface  
                      to IP DSCP.  
  
(Netgear Switch) (Config)#classofservice trust dot1p ?  
  
<cr>                Press Enter to execute the command.  
  
(Netgear Switch) (Config)#classofservice trust dot1p
```



Note: The Traffic Class value range is <0-6> instead of <0-7> because queue 7 is reserved in a stacking build for stack control, and is therefore not configurable by the user.

Traffic Shaping

This section describes the Traffic Shaping feature.

Traffic shaping controls the amount and volume of traffic transmitted through a network. This has the effect of smoothing temporary traffic bursts over time.

CLI Example

Use the *traffic-shape* command to enable traffic shaping by specifying the maximum transmission bandwidth limit for all interfaces (Global Config) or for a single interface (Interface Config).

The <bw> value is a percentage that ranges from 0 to 100 in increments of 5. The default bandwidth value is 0, meaning no upper limit is enforced, which allows the interface to transmit up to its maximum line rate.

The bw value is independent of any per-queue maximum bandwidth value(s) in effect for the interface and should be considered as a second-level transmission rate control mechanism that regulates the output of the entire interface regardless of which queues originate the outbound traffic.

Example #1 traffic-shape

```
(Netgear Switch) (Config)#traffic-shape ?  
  
<bw>                Enter the shaping bandwidth percentage from 0 to 100  
                    in increments of 5.  
  
(Netgear Switch) (Config)#traffic-shape 70 ?  
  
<cr>                Press Enter to execute the command.  
  
(Netgear Switch) (Config)#traffic-shape 70  
  
(Netgear Switch) (Config)#
```


Chapter 9

Differentiated Services

Differentiated Services (DiffServ) is one technique for implementing Quality of Service (QoS) policies. Using DiffServ in your network allows you to directly configure the relevant parameters on the switches and routers rather than using a resource reservation protocol. This section explains how to configure the 7000 Series Managed Switch to identify which traffic class a packet belongs to, and how it should be handled to provide the desired quality of service. As implemented on the 7000 Series Managed Switch, DiffServ allows you to control what traffic is accepted and what traffic is discarded.

How you configure DiffServ support on a 7000 Series Managed Switch varies depending on the role of the switch in your network:

- **Edge device.** An edge device handles ingress traffic, flowing towards the core of the network, and egress traffic, flowing away from the core. An edge device segregates inbound traffic into a small set of traffic classes, and is responsible for determining a packet's classification. Classification is primarily based on the contents of the Layer 3 and Layer 4 headers, and is recorded in the Differentiated Services Code Point (DSCP) added to a packet's IP header.
- **Interior node.** A switch in the core of the network is responsible for forwarding packets, rather than for classifying them. It decodes the DSCP code point in an incoming packet, and provides buffering and forwarding services using the appropriate queue management algorithms.

Before configuring DiffServ on a particular 7000 Series Managed Switch, you must determine the QoS requirements for the network as a whole. The requirements are expressed in terms of rules, which are used to classify inbound traffic on a particular interface. The switch software does not support DiffServ in the outbound direction.

Rules are defined in terms of classes, policies and services:

- **Class.** A class consists of a set of rules that identify which packets belong to the class. Inbound traffic is separated into traffic classes based on Layer 3 and 4 header data and the VLAN ID, and marked with a corresponding DSCP value. One type of class is supported: **All**, which specifies that every match criterion defined for the class must be true for a match to occur.
- **Policy.** Defines the QoS attributes for one or more traffic classes. An example of an attribute is the ability to mark a packet at ingress. The 7000 Series Managed Switch supports the following policy type:
Traffic Conditioning Policy - this type of policy is associated with an inbound traffic class and specifies the actions to be performed on packets meeting the class rules:

- Marking the packet with a given DSCP code point, IP precedence, or CoS
- Policing packets by dropping or re-marking those that exceed the class's assigned data rate
- Counting the traffic within the class
- **Service.** Assigns a policy to an interface for inbound traffic

CLI Example

This example shows how a network administrator can provide equal access to the Internet (or other external network) to different departments within a company. Each of four departments has its own Class B subnet that is allocated 25% of the available bandwidth on the port accessing the Internet.

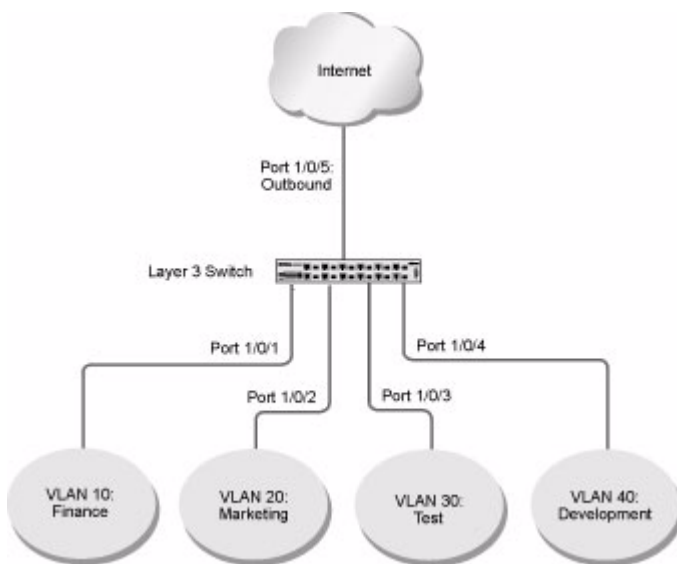


Figure 9-1

The following example configures DiffServ on a 7000 Series Managed Switch:

```

    Ensure DiffServ operation is enabled for the switch.
(Netgear Switch) #config
(Netgear Switch) (Config)#diffserv

    Create a DiffServ class of type "all" for each of the departments,
    and name them. Define the match criteria -- Source IP address --
    for the new classes.

(Netgear Switch) (Config)#class-map match-all finance_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.10.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit

(Netgear Switch) (Config)#class-map match-all marketing_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.20.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit

(Netgear Switch) (Config)#class-map match-all test_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.30.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit

(Netgear Switch) (Config)#class-map match-all development_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.40.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit

    Create a DiffServ policy for inbound traffic named
    'internet_access', adding the previously created department
    classes as instances within this policy.
    This policy uses the assign-queue attribute to put each depart-
    ment's traffic on a different egress queue. This is how the Diff-
    Serv inbound policy connects to the CoS queue settings established
    below.

(Netgear Switch) (Config)#policy-map internet_access in
(Netgear Switch) (Config policy-map)#class finance_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 1
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class marketing_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 2
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class test_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 3
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class development_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 4
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#exit
```

Attach the defined policy to interfaces 1/0/1 through 1/0/4 in the inbound direction

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/1)#exit

(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/3)#exit

(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/4)#exit
```

Set the CoS queue configuration for the (presumed) egress interface 1/0/5 such that each of queues 1, 2, 3 and 4 get a minimum guaranteed bandwidth of 25%. All queues for this interface use weighted round robin scheduling by default. The DiffServ inbound policy designates that these queues are to be used for the departmental traffic through the assign-queue attribute. It is presumed that the switch will forward this traffic to interface 1/0/5 based on a normal destination address lookup for internet traffic.

```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#cos-queue min-bandwidth 0 25 25 25 25 0 0 0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Config)#exit
```

DiffServ for VoIP Configuration Example

One of the most valuable uses of DiffServ is to support Voice over IP (VoIP). VoIP traffic is inherently time-sensitive: for a network to provide acceptable service, a guaranteed transmission rate is vital. This example shows one way to provide the necessary quality of service: how to set up

a class for UDP traffic, have that traffic marked on the inbound side, and then expedite the traffic on the outbound side. The configuration script is for Router 1 in the accompanying diagram: a similar script should be applied to Router 2.

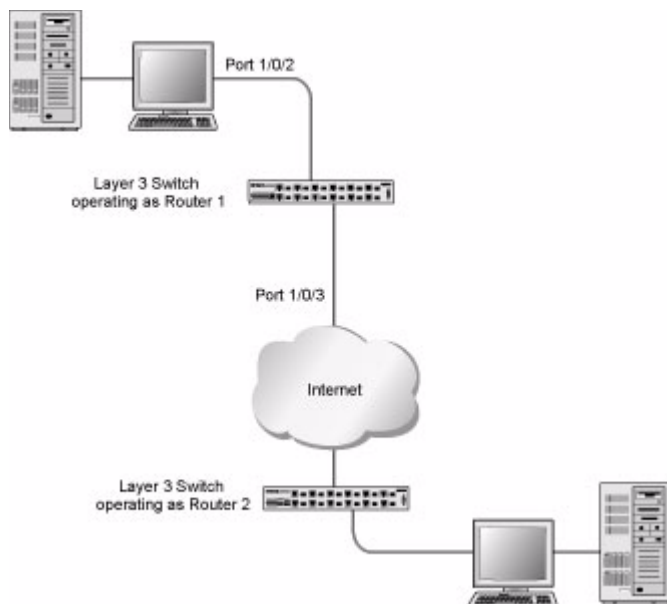


Figure 9-2

The following example configures DiffServ VoIP support:

```
Enter Global Config mode. Set queue 5 on all ports to use strict
priority mode. This queue shall be used for all VoIP packets.
Activate DiffServ for the switch.
(Netgear Switch) #config
(Netgear Switch) (Config)#cos-queue strict 5
(Netgear Switch) (Config)#diffserv

Create a DiffServ classifier named 'class_voip' and define a single
match criterion to detect UDP packets. The class type "match-
all" indicates that all match criteria defined for the class must
be satisfied in order for a packet to be considered a match.

(Netgear Switch) (Config)#class-map match-all class_voip
(Netgear Switch) (Config class-map)#match protocol udp
(Netgear Switch) (Config class-map)#exit

Create a second DiffServ classifier named 'class_ef' and define a
single match criterion to detect a DiffServ code point (DSCP) of
'EF' (expedited forwarding). This handles incoming traffic that
was previously marked as expedited somewhere in the network.

(Netgear Switch) (Config)#class-map match-all class_ef
(Netgear Switch) (Config class-map)#match ip dscp ef
(Netgear Switch) (Config class-map)#exit

Create a DiffServ policy for inbound traffic named 'pol_voip',
then add the previously created classes 'class_ef' and
'class_voip' as instances within this policy.
This policy handles incoming packets already marked with a DSCP
value of 'EF' (per 'class_ef' definition), or marks UDP packets
per the 'class_voip' definition) with a DSCP value of 'EF'. In
each case, the matching packets are assigned internally to use
queue 5 of the egress port to which they are forwarded.

(Netgear Switch) (Config)#policy-map pol_voip in
(Netgear Switch) (Config policy-map)#class class_ef
(Netgear Switch) (Config policy-class-map)#assign-queue 5
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class class_voip
(Netgear Switch) (Config policy-class-map)#mark ip-dscp ef
(Netgear Switch) (Config policy-class-map)#assign-queue 5
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#exit

Attach the defined policy to an inbound service interface.

(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in pol_voip
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Chapter 10

IGMP Snooping

This section describes the Internet Group Management Protocol (IGMP) feature: IGMPv3 and IGMP Snooping.

Overview

IGMP:

- Uses Version 3 of IGMP
- Includes snooping
- Snooping can be enabled per VLAN

CLI Examples

The following are examples of the commands used in the IGMP Snooping feature.

Example #1: Enable IGMP Snooping

The following example shows how to enable IGMP snooping.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip igmpsnooping
(Netgear Switch) (Config)#ip igmpsnooping interfacemode
(Netgear Switch) (Config)# exit
```

Example #2: show igmpsnooping

```
(Netgear Switch)      #show igmpsnooping?

<cr>                  Press Enter to execute the command.
<slot/port>          Enter interface in slot/port format.
mrouter              Display IGMP Snooping Multicast Router information.
<l-4093>             Display IGMP Snooping valid VLAN ID information.

(Netgear Switch)      #show igmpsnooping

Admin Mode..... Enable
Multicast Control Frame Count..... 0
Interfaces Enabled for IGMP Snooping..... 1/0/10
Vlans enabled for IGMP snooping..... 20
```

Example #3: show mac-address-table igmpsnooping

```
(Netgear Switch) #show mac-address-table igmpsnooping ?

<cr>                  Press Enter to execute the command.

(Netgear Switch) #show mac-address-table igmpsnooping

-----
00:01:01:00:5E:00:01:16   Dynamic   Network Assist   Fwd: 1/0/47
00:01:01:00:5E:00:01:18   Dynamic   Network Assist   Fwd: 1/0/47
00:01:01:00:5E:37:96:D0   Dynamic   Network Assist   Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FA   Dynamic   Network Assist   Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FE   Dynamic   Network Assist   Fwd: 1/0/47
```


Chapter 11

Port Security

This section describes the Port Security feature.

Overview

Port Security:

- Allows for limiting the number of MAC addresses on a given port
- Packets that have a matching MAC address (secure packets) are forwarded; all other packets (unsecure packets) are restricted
- Enabled on a per port basis
- When locked, only packets with allowable MAC address will be forwarded
- Supports both dynamic and static
- Implement two traffic filtering methods
 - Dynamic Locking - User specifies the maximum number of MAC addresses that can be learned on a port. The maximum number of MAC addresses is platform dependent and is given in the software Release Notes. After the limit is reached, additional MAC addresses are not learned. Only frames with an allowable source MAC address are forwarded.
 - Static Locking - User manually specifies a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses.
 - These methods can be used concurrently

Operation

Port Security:

- Helps secure network by preventing unknown devices from forwarding packets
- When link goes down, all dynamically locked addresses are 'freed'
- If a specific MAC address is to be set for a port, set the dynamic entries to 0, then only allow packets with a MAC address matching the MAC address in the static list
- Dynamically locked MAC addresses are aged out if another packet with that address is not seen within the age-out time. The user can set the time-out value.
- Dynamically locked MAC addresses are eligible to be learned by another port
- Static MAC addresses are not eligible for aging
- Dynamically locked addresses can be converted to statically locked addresses

CLI Examples

The following are examples of the commands used in the Port Security feature.

Example #1: show port security

```
(Netgear Switch) #show port-security ?

<cr>          Press Enter to execute the command.
all           Display port-security information for all interfaces.
<unit/slot/port> Enter interface in unit/slot/port format.
dynamic       Display dynamically locked MAC addresses.
static        Display statically locked MAC addresses.
violation     Display the source MAC address of the last packet that
              was discarded on a locked port.

(Netgear Switch) #show port-security

Port Security Administration Mode: Enabled
```

Example #2: show port security on a specific interface

```
(Netgear Switch) #show port-security 1/0/10
```

Intf	Admin Mode	Dynamic Limit	Static Limit	Violation Trap Mode
1/0/10	Disabled	600	20	Disabled

Example #3: (Config) port security

```
(Netgear Switch) (Config) #port-security ?

<cr>      Press Enter to execute the command.

(Netgear Switch) (Config) #port-security
```


Chapter 12

Traceroute

This section describes the Traceroute feature.

Use Traceroute to discover the routes that packets take when traveling on a hop-by-hop basis to their destination through the network.

- Maps network routes by sending packets with small Time-to-Live (TTL) values and watches the ICMP time-out announcements
- Command displays all L3 devices
- Can be used to detect issues on the network
- Tracks up to 20 hops
- Default UDP port used 33343 unless modified in the traceroute command



Note: You can execute Traceroute with CLI commands only—there is no Web interface for this feature.

CLI Example

The following shows an example of using the traceroute command to determine how many hops there are to the destination. The command output shows each IP address the packet passes through and how long it takes to get there. In this example, the packet takes 16 hops to reach its destination.

```
(Netgear Switch) #traceroute?
<ipaddr>      Enter IP address.

(Netgear Switch) #traceroute 216.109.118.74 ?
<cr>          Press Enter to execute the command.
<port>        Enter port no.

(Netgear Switch) #traceroute 216.109.118.74

Tracing route over a maximum of 20 hops

 1  10.254.24.1          40 ms      9 ms      10 ms
 2  10.254.253.1         30 ms      49 ms      21 ms
 3  63.237.23.33         29 ms      10 ms      10 ms
 4  63.144.4.1           39 ms      63 ms      67 ms
 5  63.144.1.141         70 ms      50 ms      50 ms
 6  205.171.21.89        39 ms      70 ms      50 ms
 7  205.171.8.154        70 ms      50 ms      70 ms
 8  205.171.8.222        70 ms      50 ms      80 ms
 9  205.171.251.34       60 ms      90 ms      50 ms
10  209.244.219.181      60 ms      70 ms      70 ms
11  209.244.11.9         60 ms      60 ms      50 ms
12  4.68.121.146         50 ms      70 ms      60 ms
13  4.79.228.2           60 ms      60 ms      60 ms
14  216.115.96.185       110 ms     59 ms      70 ms
15  216.109.120.203      70 ms      66 ms      95 ms
16  216.109.118.74       78 ms     121 ms     69 ms
```

Chapter 13

Configuration Scripting

This section describes the Configuration Scripting feature.

Overview

Configuration Scripting:

- Allows you to generate text-formatted files
- Provides scripts that can be uploaded and downloaded to the system
- Provides flexibility to create command configuration scripts
- May be applied to several switches
- Can save up to ten scripts or 500K of memory
- Provides List, Delete, Apply, Upload, Download
- Provides script format of one CLI command per line

Considerations

- Total number of scripts stored on box limited by NVRAM/FLASH size.
- Application of scripts is partial if script fails. For example, if the script executes five of ten commands and the script fails, the script stops at five.
- Scripts cannot be modified or deleted while being applied.
- Validation of scripts checks for syntax errors only. It does not validate that the script will run.

CLI Examples

The following are examples of the commands used for the Configuration Scripting feature.

Example #1: script

```
(Netgear Switch) #script ?

apply      Applies configuration script to the switch.
delete     Deletes a configuration script file from the switch.
list       Lists all configuration script files present on the switch.
show       Displays the contents of configuration script.
validate   Validate the commands of configuration script.
```

Example #2: script list and script delete

```
(Netgear Switch) #script list

Configuration Script Name      Size(Bytes)
-----
basic.scr                     93
running-config.scr            3201

2 configuration script(s) found.
1020706 bytes free.

(Netgear Switch) #script delete basic.scr

Are you sure you want to delete the configuration script(s)? (y/n) y

1 configuration script(s) deleted.
```

Example #3: script apply running-config.scr

```
(Netgear Switch) #script apply running-config.scr

Are you sure you want to apply the configuration script? (y/n) y

The systems has unsaved changes.
Would you like to save them now? (y/n) y

Configuration Saved!
```


Example #4: Creating a Configuration Script

```
(Netgear Switch) #show running-config running-config.scr

Config script created successfully.

(Netgear Switch)                               #script list

Configuration Script Name      Size(Bytes)
-----
running-config.scr           3201

1 configuration script(s) found.
1020799 bytes free.
```

Example #5: Upload a Configuration Script

```
(Netgear Switch) #copy nvram: script running-config.scr
tftp://192.168.77.52/running-config.scr

Mode..... TFTP
Set TFTP Server IP..... 192.168.77.52
TFTP Path..... ./
TFTP Filename..... running-config.scr
Data Type..... Config Script
Source Filename..... running-config.scr

Are you sure you want to start? (y/n) y

File transfer operation completed successfully.
```


Chapter 14

Outbound Telnet

This section describes the Outbound Telnet feature.

Overview

Outbound Telnet:

- Establishes an outbound telnet connection between a device and a remote host
- A telnet connection is initiated, each side of the connection is assumed to originate and terminate at a “Network Virtual Terminal” (NVT)
- Server and user hosts do not maintain information about the characteristics of each other’s terminals and terminal handling conventions
- Must use a valid IP address

CLI Examples

The following are examples of the commands used in the Outbound Telnet feature.

Example #1: show network

```
(Netgear Switch Routing) >telnet 192.168.77.151
Trying 192.168.77.151...
(Netgear Switch Routing)
User:admin
Password:
(Netgear Switch Routing)      >en
Password:

(Netgear Switch Routing)      #show network

IP Address..... 192.168.77.151
Subnet Mask..... 255.255.255.0
Default Gateway..... 192.168.77.127
Burned In MAC Address..... 00:10:18.82.04:E9
Locally Administered MAC Address..... 00:00:00:00:00:00
MAC Address Type..... Burned In
Network Configuration Protocol Current... DHCP
Management VLAN ID..... 1
Web Mode..... Enable
Java Mode ..... Disable
```

Example #2: show telnet

```
(Netgear Switch Routing)#show telnet

Outbound Telnet Login Timeout (minutes)..... 5
Maximum Number of Outbound Telnet Sessions..... 5
Allow New Outbound Telnet Sessions..... Yes
```

Example #3: transport output telnet

```
(Netgear Switch Routing) (Config)#lineconfig ?  
  
<cr>                                Press Enter to execute the command.  
  
(Netgear Switch Routing) (Config)#lineconfig  
(Netgear Switch Routing) (Line)#transport ?  
  
input                               Displays the protocols to use to connect to a  
                                   specific line of the router.  
output                              Displays the protocols to use for outgoing  
                                   connections from a line.  
  
(Netgear Switch Routing) (Line)#transport output ?  
  
telnet                              Allow or disallow new telnet sessions.  
  
(Netgear Switch Routing) (Line)#transport output telnet ?  
  
<cr>                                Press Enter to execute the command.  
  
(Netgear Switch Routing) (Line)#transport output telnet  
(Netgear Switch Routing) (Line)#
```

Example #4: session-limit and session-timeout

```
(Netgear Switch Routing) (Line)#session-limit ?  
  
<0-5>                               Configure the maximum number of outbound telnet sessions  
allowed.  
  
(Netgear Switch Routing) (Line)#session-limit 5  
(Netgear Switch Routing) (Line)#session-timeout ?  
  
<1-160>                             Enter time in minutes.  
  
(Netgear Switch Routing) (Line)#session-timeout 15
```


Chapter 15 Port Mirroring

This section describes the Port Mirroring feature.

Overview

Port Mirroring:

- Allows you to monitor network traffic with an external network analyzer
- Forwards a copy of each incoming and outgoing packet to a specific port
- Is used as a diagnostic tool, debugging feature or means of fending off attacks
- Assigns a specific port to copy all packets to
- Allows inbound or outbound packets to switch to their destination and to be copied to the mirrored port

CLI Examples

The following are examples of the commands used in the Port Mirroring feature.

Example #1: show monitor session

```
(Netgear Switch Routing) #show monitor session 1
```

Session ID	Admin Mode	Probe Port	Mirrored Port
-----	-----	-----	-----
1	Enable	1/0/8	1/0/7



Note: Monitor session ID “1” - “1” is a hardware limitation.

Example #2: show port all

```
(Netgear Switch Routing) #show port all
```

Intf	Type	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	LACP Mode
----	----	-----	-----	-----	-----	----	----
1/0/1		Enable	Auto		Down	Enable	Enable
1/0/2		Enable	Auto		Down	Enable	Enable
1/0/3		Enable	Auto		Down	Enable	Enable
1/0/4		Enable	Auto		Down	Enable	Enable
1/0/5		Enable	Auto		Down	Enable	Enable
1/0/6		Enable	Auto		Down	Enable	Enable
1/0/7	Mirror	Enable	Auto		Down	Enable	Enable
1/0/8	Probe	Enable	Auto		Down	Enable	Enable
1/0/10		Enable	Auto		Down	Enable	Enable

Example #3: show port interface

Use this command for a specific port. The output shows whether the port is the mirror or the probe

port, and what is enabled or disabled on the port.

```
(Netgear Switch Routing) #show port 0/7
```

Intf	Type	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	LACP Mode
1/0/7	Mirror	Enable	Auto		Down	Enable	Enable

```
(Netgear Switch Routing) #show port 0/8
```

Intf	Type	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	LACP Mode
----	----	-----	-----	-----	-----	----	----
1/0/8	Probe	Enable	Auto		Down	Enable	Enable

Example #4: (Config) monitor session 1 mode

To set up port mirroring, specify the monitor session, then the mode.

```
(Netgear Switch Routing)(Config)#monitor?
```

```
session      Configure port mirroring.
```

```
(Netgear Switch Routing)(Config)#monitor session?
```

```
<1-1>      Session number.
```

```
(Netgear Switch Routing)(Config)#monitor session 1?
```

```
destination  Configure the probe interface.
```

```
mode        Enable/Disable port mirroring session.
```

```
source       Configure the source interface.
```

```
(Netgear Switch Routing)(Config)#monitor session 1 mode?
```

```
<cr>      Press Enter to execute the command.
```

```
(Netgear Switch Routing)(Config)#monitor session 1 mode
```

Example #5: (Config) monitor session 1 source interface

Specify the source (mirrored) ports and destination (probe) port.

```
(Netgear Switch Routing)(Config)#monitor session 1 source?
interface      Configure interface.

(Netgear Switch Routing)(Config)#monitor session 1 source interface?
<slot/port>      Enter the interface.
(Netgear Switch Routing)(Config)#monitor session 1 source interface 0/7

(Netgear Switch Routing)(Config)#monitor session 1 destination?
interface      Configure interface.

(Netgear Switch Routing)(Config)#monitor session 1 destination interface?
<slot/port>      Enter the interface.
(Netgear Switch Routing)(Config)#monitor session 1 destination interface 0/8
```

Example #6: (Interface) port security

```
(Netgear Switch Routing)(Interface 0/7)#port-security ?

<cr>      Press Enter to execute the command.
mac-address      Add Static MAC address to the interface.
max-dynamic      Set Dynamic Limit for the interface.
max-static       Set Static Limit for the interface.

(Netgear Switch Routing)(Interface 0/7)#port-security max-static ?

<0-20>      Set Static Limit for the interface.

(Netgear Switch Routing)(Interface 0/7)#port-security max-static 5
(Netgear Switch Routing)(Interface 0/7)#port-security max-dynamic 10
```

Chapter 16

Simple Network Time Protocol (SNTP)

This section describes the Simple Network Time Protocol (SNTP) feature.

Overview

SNTP:

- Used for synchronizing network resources
- Adaptation of NTP
- Provides synchronized network timestamp
- Can be used in broadcast or unicast mode
- SNTP client implemented over UDP which listens on port 123

CLI Examples

The following are examples of the commands used in the SNTP feature.

Example #1: show sntp

```
(Netgear Switch Routing) #show sntp ?  
  
<cr>      Press Enter to execute the command.  
client    Display SNTP Client Information.  
server    Display SNTP Server Information.
```

Example #2: show sntp client

```
(Netgear Switch Routing) #show sntp client

Client Supported Modes:    unicast broadcast
SNTP Version:             4
Port:                    123
Client Mode:              unicast
Unicast Poll Interval:    6
Poll Timeout (seconds):   5
Poll Retry:               1
```

Example #3: show sntp server

```
(Netgear Switch Routing) #show sntp server

Server IP Address:        81.169.155.234
Server Type:              ipv4
Server Stratum:           3
Server Reference Id:      NTP Srv: 212.186.110.32
Server Mode:              Server
Server Maximum Entries:   3
Server Current Entries:   1

SNTP Servers
-----

IP Address:               81.169.155.234
Address Type:             IPV4
Priority:                  1
Version:                  4
Port:                     123
Last Update Time:         MAY 18 04:59:13 2005
Last Attempt Time:        MAY 18 11:59:33 2005
Last Update Status:       Other
Total Unicast Requests:   1111
Failed Unicast Requests:  361
```

Example #4: Configure SNTP

Netgear switches do not have a built-in real-time clock. However, it is possible to use SNTP to get the time from a public SNTP/NTP server over the Internet. You may need permission from those public time servers. The following steps configure SNTP on the switch:

1. Configure the SNTP server IP address. The IP address can be either from the public NTP server or your own. You can search the Internet to locate the public server. The servers available could be listed in domain-name format instead of address format. In that case, use the ping command on the PC to find the server's IP address. The following example configures the SNTP server IP address to 208.14.208.19.

```
(Netgear Switch) (Config)#sntp server 208.14.208.19
```

2. After configuring the IP address, enable SNTP client mode. The client mode may be either broadcast mode or unicast mode. If the NTP server is not your own, you must use unicast mode.

```
(Netgear Switch) (Config)#sntp client mode unicast
```

3. Once enabled, the client will wait for the polling interval to send the query to the server. The default value is approximately one minute. After this period, issue the show command to confirm the time has been received. The time will be used in all logging messages.

```
(Netgear Switch) #show sntp server
Server IP Address:          208.14.208.19
Server Type:                ipv4
Server Stratum:             4
Server Reference Id:        NTP Srv: 208.14.208.3
Server Mode:                Server
Server Maximum Entries:     3
Server Current Entries:     1
SNTP Servers
-----
IP Address: 208.14.208.19
Address Type: IPV4
Priority: 1
Version: 4
Port: 123
Last Update Time: Mar 26 03:36:09 2006
Last Attempt Time: Mar 26 03:36:09 2006
Last Update Status: Success
Total Unicast Requests: 2
Failed Unicast Requests: 0
```


Chapter 17

Pre-Login Banner

This section describes the Pre-Login Banner feature.

Overview

Pre-Login Banner:

- Allows you to create message screens when logging into the CLI Interface
- By default, no Banner file exists
- Can be uploaded or downloaded
- File size cannot be larger than 2K

The Pre-Login Banner feature is only for the CLI interface.

CLI Example

To create a Pre-Login Banner, follow these steps:

1. On your PC, using Notepad create a banner.txt file that contains the banner to be displayed.

`Login Banner - Unauthorized access is punishable by law.`

2. Transfer the file from the PC to the switch using TFTP

```
(Netgear Switch Routing) #copy tftp://192.168.77.52/banner.txt
nvram:clibanner

Mode..... TFTP
Set TFTP Server IP..... 192.168.77.52
TFTP Path..... ./
TFTP Filename..... banner.txt
Data Type..... Cli Banner

Are you sure you want to start? (y/n) y

CLI Banner file transfer operation completed successfully!

(Netgear Switch Routing) #exit

(Netgear Switch Routing) >logout

Login Banner - Unauthorized access is punishable by law.
User:
```



Note: The command “no clibanner” removes the banner from the switch.

Chapter 18

Syslog

This section provides information about the Syslog feature.

Overview

Syslog:

- Allows you to store system messages and/or errors
- Can store to local files on the switch or a remote server running a syslog daemon
- Method of collecting message logs from many systems

Persistent Log Files

- Currently three - one for each of the last three sessions
- Each log has two parts:
 - Start up log is the first 32 messages after system startup
 - Operational log is the last 32 messages received after the startup log is full
- Files are stored in ASCII format
 - slog0.txt - slog2.txt
 - olog0.txt - olog2.txt

Where 0 is for the boot, 1 is for the last boot, 2 is for the boot before that, and the third one falls off.
- Can be saved to local server to monitor at a later point in time

Interpreting Log Files

<130> JAN 01 00:00:06 0.0.0.0-1 UNKN [0x800023]: bootos.c(386) 4 %% Event (0xaaaaaaaa)

The diagram shows a log entry: <130> JAN 01 00:00:06 0.0.0.0-1 UNKN [0x800023]: bootos.c(386) 4 %% Event (0xaaaaaaaa). Arrows point from labels A through I to the following fields: A points to <130>, B points to 00:00:06, C points to 0.0.0.0-1, D points to UNKN, E points to [0x800023], F points to bootos.c(386), G points to 4, H points to %% Event, and I points to (0xaaaaaaaa).

- A. Priority
- B. Timestamp
- C. Stack ID
- D. Component Name
- E. Thread ID
- F. File Name
- G. Line Number

CLI Examples

The following are examples of the commands used in the Syslog feature.

Example #1: show logging

```
(Netgear Switch Routing) #show logging

Logging Client Local Port      :    514
CLI Command Logging           :    disabled
Console Logging               :    disabled
Console Logging Severity Filter :    alert
Buffered Logging              :    enabled

Syslog Logging                :    enabled

Log Messages Received         :    66
Log Messages Dropped         :    0
Log Messages Relayed         :    0
Log Messages Ignored         :    0
```

Example #2: show logging buffered

```
(Netgear Switch Routing) #show logging buffered ?

<cr>    Press Enter to execute the command.

(Netgear Switch Routing) #show logging buffered

Buffered (In-Memory) Logging      :    enabled
Buffered Logging Wrapping Behavior :    On
Buffered Log Count                :    66

<1> JAN 01 00:00:02 0.0.0.0-0 UNKN[268434944]: usmdb_sim.c(1205) 1 %% Error 0
(0x0)
<2> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(487) 2 %% Event
(0xaaaaaaaa)
<6> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(531) 3 %% Starting
code...
<6> JAN 01 00:00:16 0.0.0.0-3 UNKN[251627904]: cda_cnfg.c(383) 4 %% CDA:
Creating new STK file.
<6> JAN 01 00:00:39 0.0.0.0-3 UNKN[233025712]: edb.c(360) 5 %% EDB Callback:
Unit Join: 3.
<6> JAN 01 00:00:40 0.0.0.0-3 UNKN[251627904]: sysapi.c(1864) 6 %% File
user_mgr_cfg: same version (6) but the sizes (2312->7988) differ
```

Example #3: show logging traplogs

```
(Netgear Switch Routing) #show logging traplogs ?  
  
<cr>      Press Enter to execute the command.  
  
(Netgear Switch Routing) #show logging traplogs  
  
Number of Traps Since Last Reset.....          6  
Trap Log Capacity.....                        256  
Number of Traps Since Log Last Viewed.....      6  
  
Log System Up Time          Trap  
---- -  
0  0 days 00:00:46          Link Up: Unit: 3 Slot: 0 Port: 2  
1  0 days 00:01:01          Cold Start: Unit: 0  
2  0 days 00:21:33          Failed User Login: Unit: 1 User ID: admin  
3  0 days 18:33:31          Failed User Login: Unit: 1 User ID: \  
4  0 days 19:27:05          Multiple Users: Unit: 0      Slot: 3 Port: 1  
5  0 days 19:29:57          Multiple Users: Unit: 0      Slot: 3 Port: 1
```

Example 4: show logging hosts

```
(Netgear Switch Routing) #show logging hosts ?  
  
<cr>      Press Enter to execute the command.  
  
(Netgear Switch Routing) #show logging hosts  
  
Index      IP Address      Severity      Port      Status  
-----  
1          192.168.21.253    critical      514      Active
```

Example #5: logging port configuration

```
(Netgear Switch Routing)      #config

(Netgear Switch Routing) (Config)#logging ?

buffered          Buffered (In-Memory) Logging Configuration.
cli-command       CLI Command Logging Configuration.
console           Console Logging Configuration.
host              Enter IP Address for Logging Host
syslog            Syslog Configuration.

(Netgear Switch Routing) (Config)#logging host ?

<hostaddress>     Enter Logging Host IP Address
reconfigure       Logging Host Reconfiguration
remove            Logging Host Removal

(Netgear Switch Routing) (Config)#logging host 192.168.21.253 ?

<cr>              Press Enter to execute the command.
<port>            Enter Port Id

(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 ?

<cr>              Press Enter to execute the command.
<severitylevel>   Enter Logging Severity Level (emergency|0, alert|1,
critical|2, error|3, warning|4, notice|5, info|6, debug|7).

(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 1 ?

<cr>              Press Enter to execute the command.

(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 1

(Netgear Switch Routing) #show logging hosts
```

Index	IP Address	Severity	Port	Status
1	192.168.21.253	alert	4	Active

